



المركز العربي
للبحوث القانونية
والقضائية

د. منى الاشقر جبور

د. محمود جبور

أبحاث ودراسات (5)

البيانات الشخصية والقوانين العربية:
الهمّ الأمني وحقوق الأفراد

تأليف

د. منى الاشقر جبور

د. محمود جبور

المركز العربي للبحوث القانونية والقضائية

مجلس وزراء العدل العرب

جامعة الدول العربية

الطبعة الأولى

بيروت - لبنان

2018

جدول المحتويات

استهلال

تندرج هذه الدراسة، في إطار جهود مركز البحوث والدراسات القانونية والقضائية، الرامية إلى مقاربة البعد العالمي، والعابر للحدود، لموضوع حماية البيانات الشخصية، وإيمانه بضرورة العمل على المستوى العربي، لإيجاد الرد المناسب، على التهديدات والمخاطر، التي باتت تهدد امن الدول والأفراد في آن، لاسيما بعد الفضائح الكبرى، التي أبرزت مخاطر التجسس، الذي تقوم به بعض الدول، وبعض الشركات الكبرى، عبر رصد حركة مستخدمي الأنترنت، وجمع بياناتهم الشخصية، والاعتداء على حقهم في الخصوصية، ما يؤسس لاعتداء على حقوق وحريات، المواطنين العرب، ويهدد الثقة اللازمة، لعملية الانخراط في الاقتصاد الرقمي.

كما إنها تضاف إلى لائحة من الدراسات، التي تؤشر إلى سعي دؤوب من قبل الجامعة العربية، لحث أعضائها، على إقرار اطر تشريعية ملائمة لعصر التقنيات المتطورة، التزاما بمقررات القمة العالمية لمجتمع المعلومات، بشقيها جنيف وتونس، وبنتائج القمة التي عقدت في البرازيل[1]، حول حوكمة الإنترنت، بعد ما عرف بفضيحة سنودين، وتنبه دول العالم، إلى أهمية التعاون بينها، لمواجهة المخاطر المرتبطة بالتجسس والتنصت، إضافة إلى ضرورة المحافظة على ديمقراطية الإنترنت، وسلامة الفضاء السيبراني.

ولحماية البيانات الشخصية، كما هو معلوم، دور حاسم في بناء بيئة مؤاتية، لتأمين سلامة هذا الفضاء، ودعم استقراره، لان أمن البيانات، جزء من الأمن السيبراني. وعليه، فان هذه الحماية تدعم بناء الثقة، وتساهم في تشجيع التجارة والخدمات الإلكترونية.

[1] Un sommetinédit au Brésilsur la "gouvernance du net"
https://www.francetvinfo.fr/sciences/high-tech/un-sommet-inedit-au-bresil-sur-la-gouvernance-du-net_1685949.html

ويشكل اعتماد إطار قانوني وتنظيمي، لحماية البيانات الشخصية، بشكل خاص، وسيلة لتحقيق الانسجام، مع توجهات المنظمات والهيئات الدولية، كمنظمة التعاون الاقتصادي والتنمية، والاتحاد الأوروبي، اللذين أصدرا عددا من التوجيهات، والإرشادات، والقرارات، حول مبادئ حماية البيانات الشخصية.

ففي ظل العولمة، وسهولة الحصول على البيانات وتداولها، تتضاعف أهمية إرساء نظام فاعل للحماية، وفرض إجراءات قانونية صارمة، ضد إساءة استخدام البيانات الشخصية، والاعتداء على الخصوصية. ولا بد من الالتزام بتطبيق ومواكبة أرقى المعايير، في هذا المجال، حفاظا على إمكانات وفرص الإفادة، مما يمكن أن تقدمه التقنيات الحديثة في معالجة البيانات، سواء على مستوى تطوير الاقتصاد، أو على مستوى الإنماء الاجتماعي والثقافي.

ولان الانسجام على المستوى القانوني، حاجة ملحة في المواجهة، كان لا بد من دراسة مقارنة، تبحث في مدى تقارب القوانين العربية الخاصة بحماية البيانات الشخصية، فيما بينها، من جهة أولى، ومدى انسجامها مع القوانين الدولية، والتوصيات المعتمدة عالميا، من جهة ثانية، عبر تبيان نقاط الالتقاء والاختلاف، أينما وجدت.

المقدمة

استتبع التحول إلى الرقمية، إنتاج كميات هائلة من البيانات الشخصية، وتعاظمت المخاطر التي تترتب على إدارتها، واستثمارها.

حجم غير مسبوق من البيانات

أشارت الإحصاءات الصادرة العام المنصرم، إلى وجود اكثر من نصف سكان العالم على الإنترنت[2]، وترافق هذا التصاعد في إعداد مستخدمي الإنترنت، مع تصاعد نسبة القلق. فالانتقال السريع إلى استخدام تقنيات المعلومات والاتصالات، والتحولات التقنية المتعاظمة، لم يسمحا بمواكبة فاعلة لمخاطرها، سواء أكان من قبل الحكومات وصناع السياسات، إم من قبل الأفراد.

لقد انتج العالم خلال العام 2017، معدلات غير مسبوقة من البيانات، تجاوز بضخامتها ما انتج على امتداد كامل تاريخ البشرية، ما فرض تنبه المعنيين في القطاعين العام والخاص، إلى أهمية إدارتها بشكل فاعل، مع مراعاة الجوانب التقنية، والاقتصادية، والإدارية، والقانونية، التي تترتب على ذلك. فمع الانتقال إلى الرقمية، تحولت البيانات إلى قيمة لا تقدر بثمن، ومورد لاقتصاد المعرفة.

وفي هذا السياق، تنشر الشركات العاملة، في مجال تقنيات المعلومات، بشكل مستمر، عدد المُستخدمين الموجودين لديها، كما لا تتأخر شركات الإحصاء، عن إصدار تقاريرها حول هذا الموضوع، بهدف تأمين المعلومات اللازمة، للشركات وأصحاب المواقع المختلفة، كي يتمكنوا من وضع خطط انتشارهم، والترويج لمنتجاتهم، وتسويق خدماتهم.

[2] - https://wearesocial.com/blog/2018/01/global-digital-report-2018
DIGITAL IN 2018: WORLD’S INTERNET USERS PASS THE 4 BILLION MARK - Well over half of the world’s population is now online, with the latest data showing that nearly a quarter of a billion new users came online for the first time in 2017.

وإذ يصل حجم الأشخاص، الذين يستخدمون شبكة الفيسبوك، إلى ما يفوق الملياري شخص[3]، ويصل العدد إلى 800 مليون، على انستغرام، وإلى أكثر من مليار على واتساب، يتجاوز حجم البيانات التي تنتج عن هذا الاستخدام، 2.5 إكسا بايت ExaByte في الدقيقة الواحدة تقريباً.

وتعتبر تطبيقات المحادثات الفورية، مصدراً آخراً لإنتاج البيانات، حيث يتم إرسال أكثر من 527 ألف صورة، بواسطة السناب شات، في الدقيقة، وتحصل منصّة لينكدإن Linked in على أكثر من 120 حساب جديد، ويرسل مستخدمو تويتر 456 ألف تغريده، بينما يُعالج غوغل أكثر من 3.6 مليون عملية بحث، وتجني أمازون أكثر من ثلاثمائة ألف دولار أمريكي من المبيعات، التي تجري في الدقيقة الواحدة على الإنترنت، هذا، عدا عن الحجم الهائل للاستثمارات، التي تقوم بها الدول في مجال البيانات الضخمة[4].

تلك الأرقام الهائلة تُفسّر اتّجاه الشركات الكُبرى نحو الاستثمار في البيانات الشخصية، فهي ثروة تعيش عليها الشركات، التقنية منها، والتقليدية، نتيجة استخدامها في مجال تطوير المنتجات، والإعلانات، عبر تحليلها، وتحليل ميول الأشخاص الطبيعيين، وتحديد حاجاتهم، وعاداتهم الاستهلاكية، واهتماماتهم.

وفي المقابل، تزداد ظاهرة دفق المعلومات على الإنترنت، بازدياد عدد الأجهزة الموصولة بها، وتعدد وسائل تخزينها؛ كالأقراص الصلبة، وأنظمة الحوسبة السحابية، كما يتنوع استخدامها، وتتنوع التطبيقات التي تهندس بناء على كيفية تميّرها، والإفادة منها لتقديم الخدمات. علماً، أن القسم الأكبر منها، يتم جمعه دون علم الشخص المعني؛ أي صاحب البيانات.

---

[3] - https://blog.statusbrew.com/social-media-statistics-2018-for-business/

[4] - Big Data Statistics & Facts for 2017
https://www.waterfordtechnologies.com/big-data-interesting-facts/

فالسيارات الذكية، مثلا، تجمع كما هائلا من البيانات[5]، غالبا دون موافقة مستخدمها، لاسيما منها، تلك التي يتم استئجارها من الوكالات المتخصصة في هذا المجال، حيث يكون أول سائق استخدمها، قد وافق على شروط الاستخدام، دون علم السائقين، الذين يتولون قيادتها فيما بعد، بما وافق على كشفه من البيانات. وهنا لا يجب أن يغيب عن البال، جهاز الهاتف الذي تدمج وظائفه بنظام السيارة، والذي يمكن السيطرة من خلاله، على وسائل الترفيه فيها، ونظام الملاحة على الشاشة، واستخدام الرسائل النصية والمكالمات.

أما المثال الآخر، فهو الأنظمة العاملة في مجال التحويلات المالية والاستثمارات، حيث تسجل حركة كل عميل، وتجمع بياناته الشخصية، بأدق تفاصيلها، وذلك بهدف إتاحة إمكانية إثبات صحة أية عملية قد يقوم بها، وتأمين كشف كامل له، في حال طلب ذلك.

على خط متصل، يزداد بروز تصاعد تأثير الذكاء الاصطناعي، على شبكات وخدمات الاتصالات، وتزداد معه أساليب، جمع البيانات، وتحليلها، وتقاطعها، بهدف استثمارها، في مجالات عديدة ومختلفة.

تحول في نماذج العمل

لقد بات واضحا اليوم، إن البيانات الشخصية، هي عصب شديد الأهمية في الاقتصاد الرقمي، وفي التنمية. فهي التي تغذي الابتكار في معظم القطاعات الصناعية، والتجارية، والخدماتية. كما تساهم عمليات معالجتها، في تحسين الأداء والإنتاجية، في قطاعات الدولة كافة، بما يساعد على التصدي للتحديات، المتعلقة بإدارة شؤون الأجهزة الحكومية، والمواطنين، والمشاكل المتصلة بصحة الإنسان، وسلامة البيئة، ومحاربة العديد من معوقات التنمية، وتطوير الموارد البشرية.

[5] - Connected cars will send 25 gigabytes of data to the cloud every hour
https://qz.com/344466/connected-cars-will-send-25-gigabytes-of-data-to-the-cloud-every-hour/

على خط متصل، برزت أهمية الإدارة الفاعلة لهذه القيمة، التي تمثلها البيانات الشخصية، على كيفية تطوير الأنظمة والتطبيقات، سواء لتحقيق التنمية، وبلوغ مستوى أعلى من الرفاه الإنساني، وتجويد نوعية الحياة، أو لتحقيق الأرباح الاقتصادية، فبلغت أرباح فيسبوك 16 مليار دولار، بينما تجاوزت أرباح محرك البحث غوغل، المئة مليار[6].

وهكذا، تتحرك الشركات التي أدركت أن ذهب العصر هو البيانات الشخصية، ضمن إطار تنظيمي، يؤثر في أساليب وطرق عملها، في جمع البيانات الشخصية، ومعالجتها، وأدارتها، والإشراف عليها، واستثمارها، بما يعود عليها بالأرباح، ويساعدها في الوصول إلى أسواق جديدة.

ففي عصر البيانات الكبيرة، وربطها، وتقييمها، تأخذ البيانات الشخصية مكانا أكثر أهمية، بحيث تحولت إلى محور النماذج الاقتصادية، والتجارية، والإدارية الجديدة. وقد أثرت أساليب وطرق معالجة هذه البيانات، في أساليب الإنتاج، واستراتيجياته. ولم تعد الشركات التقليدية، التي لا تتعامل مع معالجة البيانات، قادرة على المنافسة، أو حتى على الاستمرار، ما لم تتحول هي الأخرى، نحو هذه المعالجة.

وترتكز النماذج الاقتصادية الجديدة، بشكل واضح، على كيفية معالجتها للبيانات الشخصية، فإما أن تجمعها، وتحللها، وتستثمر فيها مباشرة، عبر بيعها، أو بيع نتائج هذه التحليلات، وإما أن تتيح حق الوصول إليها للأشخاص المعنيين، وإما أن تطور خدمات جديدة، مبنية على أساس حاجات تؤشر إليها هذه البيانات.

وفي الاقتصاد المعولم، لا مصلحة للمؤسسات والشركات، أيا كانت جنسيتها، في الخروج عن النماذج، والأطر التنظيمية والقانونية الدولية، المعتمدة من قبل زبائنها،

---

[6] - Facebook : 16 milliards de dollars de bénéfices en 2017
https://www.nextinpact.com/news/106065-facebook-16-milliards-dollars-benefices-en-2017.htm
* Le géant d'Internet a passé la barre des 100 milliards de dollars de revenus annuels.
https://www.lesechos.fr/01/02/2018/lesechos.fr/0301241341612_google---le-chiffre-d-affaires-progresse-mais-les-couts-bondissent.htm

أو منافسيها، أو مقدمي الخدمات المنتشرين حول العالم.

أما المعيار الأساس، هنا، فهو القدرة على تحديد مكان البيانات، وحمايتها، وأدارتها، بغض النظر عن البنية التحتية، التي يستخدمها صاحب البيانات، سواء أكانت على الموقع، أو في السحابة الإلكترونية، أو في الاثنين معا.

على المستوى العربي، انتشر استخدام تقنيات المعلومات والاتصالات، وتعددت استعمالات أجهزة الاتصال، ودخلت الرقمية إلى قطاعات كثيرة، في مقدمها، الخدمات المالية والمصرفية. ولعل أبرز الأمور التي تسجل هنا، هي توجه العديد من الحكومات العربية، نحو تفعيل الاقتصاد، من خلال تنمية الاقتصاد الرقمي.

وبالفعل، فقد تحول العديد منها، إلى تطوير خدمات الإنترنت، والبنية التحتية للاتصالات، وتطوير رأس المال البشري، وتأمين الاعتماد على الحكومة الإلكترونية، كوسيلة وغاية للتنمية، وكمؤشر عليها. كما انشأ عدد منها، كمصر، والإمارات، مدنا ذكية، في سعي منه إلى تحقيق التنمية المستدامة، والإفادة من تقنيات المعلومات والاتصالات، لجذب الاستثمارات، وتحريك عجلة الانخراط في مجتمع المعرفة.

وبحسب ما ورد، في تقرير يصدر دوريا عن الأمم المتحدة، تحرز الدول العربية تقدما، باتجاه الاعتماد على الحكومة الإلكترونية، لاسيما منها، دول التعاون الخليجي، حيث برزت الإمارات العربية المتحدة، وقطر، والسعودية، والكويت، والبحرين، ضمن المراكز الخمسين الأولى، على مستوى العالم [7].

كما سجلت المغرب، والإمارات، والسعودية، وتونس، ضمن الدول التي تبذل جهودا، في مجال التواصل مع المواطنين، والمعلومات المتاحة للعموم، حول الصحة، والرعاية الاجتماعية، والعمل، وغيرها.

---

[7] - https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016

الدولة والبيانات الشخصية

الفرد عماد المجتمع، وهويته جزء من شخصيته، وأساس في اكتساب الحقوق، وإقرار الواجبات، واستقرار المعاملات. لذلك، حرصت الدول منذ نشأتها، على الاهتمام بالملفات الشخصية، والإحصاء، والقيود الثبوتية؛ كالهوية، وجواز السفر، والإقامة، وإجازة ممارسة مهنة معينة، وذلك، في إطار تنظيمي وقانوني، تحدد عبره، القواعد التي تعطى على أساسها الجنسية، أو تمنع ممارسة بعض الحقوق؛ كالحقوق المدنية، أو السياسية، في حال ارتكاب الشخص لأنواع من الجرائم، تعتبر خطرة على استقرار المجتمع.

ويتم كل ذلك، وفقا لمندرجات سجلات رسمية، تديرها الإدارات الحكومية، وتسجل فيها بيانات شخصية، كالاسم، ومحل الإقامة والولادة، وتاريخ الميلاد، واسم العائلة، الخ... وتستخدم هذه السجلات أيضا، للتمييز بين المواطن، والأجنبي، وتحديد الحالة القانونية للمقيم. وتسجل في هذا المجال، أهمية احتفاظ أجهزة الأمن، والسلطات القضائية، بسجلات المخالفات، والجرائم، التي تسمح للأجهزة المعنية، بمتابعة المرتكبين، وحماية المجتمع منهم، ما يجعل عدد السجلات لدى الإدارات الحكومية، تتكاثر وتتنوع.

وكان جمع هذه البيانات، يتم بإعلان إرادي من الأفراد، رغبة منهم في اكتساب وضع قانوني، وإيجاد قيود تثبت حقوقهم، وانتماءاتهم الوطنية والعائلية، فيتم تدوينها من قبل الموظف الرسمي يدويا، على الورق، وتكون مراجعتها، أو الحصول عليها، منظمة بحيث لا تكشف إلا لأصحاب العلاقة، وللأجهزة المسؤولة في الدولة، وبطلب رسمي، ولأهداف واضحة.

إلا أن التحول إلى الرقمية، جعل هذه القيود، تتخذ ركيزة جديدة، ذات طبيعة مختلفة، تتيح مجال الاحتفاظ بها، وإعداد نسخ منها، وتوزيعها، وتبادلها، بعدد من

الوسائل، والوسائط المختلفة والمتنوعة، كالأقراص الصلبة الداخلية أو الخارجية، والحوسبة السحابية. وقد ساهم هذا الأمر، في جذب اهتمام الدول، نحو مراقبة حركة الاتصالات، ومستخدمي الإنترنت.

فالدول عامة، تحتاج إلى جمع البيانات الشخصية، حتى الحساسة منها، على الإنترنت، ووسائل الاتصال، والأجهزة المختلفة، للقيام بمهماتها كسلطة عامة، وكمسؤولة عن الاستقرار والأمن الاجتماعيين، في مواجهة أية تهديدات ومستجدات، كما هو حاصل اليوم مثلا، مع مكافحة الإرهاب، وتعقب الإرهابيين والمجرمين، عبر الإنترنت.

وبالفعل، فقد لجأت دول عديدة، في إطار تحصينها للأمن القومي، إلى تشديد الرقابة على المشتبه بهم، من خلال رصد حركة اتصالاتهم، وتعقب أجهزتهم المتصلة بالإنترنت، كما طلبت من شركات الاتصال، الاحتفاظ ببيانات الاتصال، لمدة محددة، تختلف بين بلد وآخر.

وكان هذا التحول الرقمي، الذي فتح مجالات للرقابة، إضافة إلى بروز بوادر مخاطر معالجة البيانات الشخصية إلكترونياً، منذ أواخر الستينيات من القرن الماضي، وصولا إلى الثمانينيات، قد دفع بعض الدول الأوروبية، إلى إطلاق عملية قوننة، تهدف إلى تنظيم عملية استخدام البيانات الشخصية، من قبل الإدارات الحكومية، والشركات الكبرى. فإضافة إلى القوانين التي أقرت في النمسا، والدانمارك، وفرنسا، وألمانيا، أدخلت إسبانيا، والبرتغال، والنمسا، الحق في حماية البيانات الشخصية، بين الحقوق الأساسية المحمية بالدستور[8].

ويعود هذا الاهتمام الذي أولته أوروبا، عامة، لحماية البيانات، في الأساس، إلى الخوف من جمع هذه البيانات، ومعالجتها بشكل مؤذ، يساهم في تدخل الدولة،

[8] - ORIGINS AND HISTORICAL CONTEXT OF DATA PROTECTION LAW By Sian Rudgard, Legal Director https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf

بشكل غير مبرر، في الحياة الخاصة للمواطنين، وفي تصنيفهم ضمن لوائح، على غرار ما حصل أيام الأنظمة النازية والفاشية.

وأضيف إلى هذا الخوف، واقع آخر، هو دخول القطاع الخاص، إلى مجال الاعتداءات على حقوق الأشخاص وحرياتهم، نتيجة لإمكانية الوصول على الإنترنت، إلى ملايين المعلومات الخاصة، مقابل دفع مبلغ من المال، واستخدام العديد منها، ليس فقط في الوصول إلى الأشخاص، واستهدافهم بالإعلانات الترويجية، وإنما أيضا، في عمليات احتيال مالية ومصرفية[9]، واعتداءات على الأموال والأشخاص.

وغني عن القول، إن هذه الممارسات، تشكل اتجارا غير مشروع، وغير مسبوق، بالبيانات الشخصية، كأسماء الأشخاص، وعناوينهم، وأرقام حساباتهم المصرفية، أو بطاقاتهم الصحية، التي تجمع بطريقة غير شرعية، عن مواقع الإنترنت، ما يمثل، تهديدا مباشرا، للأمن الاجتماعي، والشخصي للأفراد.

في هذا الإطار، نعرض في الفصل الأول، لارتباط الحق في الخصوصية بحماية البيانات الشخصية، وفي الفصل الثاني، للقوانين العربية الخاصة بحماية البيانات، على ضوء التوصيات والقوانين الدولية، والأوروبية.

[9] - Un trafic de données confidentielles fait scandale en Allemagne
http://www.lemonde.fr/technologies/article/2008/08/21/un-trafic-de-donnees-confidentielles-fait-scandale-en-allemagne_1086275_651865.html#bRdMTKqU4f8ECYuU.99
http://www.lemonde.fr/technologies/article/2008/08/21/un-trafic-de-donnees-confidentielles-fait-scandale-en-allemagne_1086275_651865.html

الفصل الأول

حماية البيانات الشخصية والحق في الخصوصية

حماية البيانات الشخصية

تعتبر حماية البيانات الشخصية، كأساس في حماية الخصوصية، من اهم عناصر بناء الثقة، في الفضاء السيبراني، والاستخدام الآمن لتقنيات المعلومات والاتصالات، لاسيما في النشاط الاقتصادي، والإنمائي.

ففي دراسة نشرت العام الماضي، في الولايات المتحدة الأميركية، حول الأميركيين والأمن السيبراني، عبر العديد منهم عن عدم ثقتهم بالمؤسسات الحديثة، لناجية حماية بياناته الشخصية[10]. ويدعم هذا الأمر، عدد الاعتداءات على الأنظمة المعلوماتية، وحالات تسرب البيانات الشخصية، سواء عبر اختراقات البريد الإلكتروني[11]، أو سرقة بيانات شركات تقدم خدمات عبر الإنترنت[12]، أو التلاعب بحسابات على مواقع التواصل الاجتماعي[13].

وتعود جذور عدم الثقة، إلى أسباب عديدة، ليس أقلها: حقيقة حدوث ما يقارب الـ 3700 اعتداء، على الأنظمة المعلوماتية، في كل ثانية. علما، أن 91 بالمئة، من حالات تسرب وانكشاف المعلومات، كان بالإمكان تجنبها، لو اتخذت الشركات

[10] - Americans and Cybersecurity Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives
http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[11] - Every single Yahoo account was hacked - 3 billion in all
https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

[12] - Uber admits covering up data hack that hit 57m users and drivers
http://www.france24.com/en/20171122-uber-admits-covering-hacking-affecting-57m-users-drivers

[13] - Facebook says 126 million Americans may have been exposed to Russia-linked US election posts
https://www.independent.co.uk/news/world/americas/us-politics/facebook-russia-adverts-americans-exposed-trump-us-election-2016-millions-a8028526.html

المعنية إجراءات الحماية الكافية[14].

يضاف إلى ذلك، عدم وجود تشريع أميركي موحد لحماية البيانات. فالقوانين التي تقرها الولايات الأميركية المختلفة[15]، والتي تفرض إبلاغ أصحاب البيانات، عن الاختراقات التي تحصل، وعن سرقة بياناتهم الشخصية، لا تقدم حماية فاعلة، لاسيما وأن معظم هذه الاختراقات، وحالات تسرب وسرقة البيانات، لا تنكشف إلا بعد مضي فترة عليها، يكون قد تم خلالها، سواء سرقة هوية الأشخاص المعنيين، أو التلاعب بحساباتهم، وربما التعرض لسلامتهم الجسدية، والنفسية.

- **أوروبا نموذجاً**

لكن الإشارة واجبة هنا، إلى إدخال القواعد الأوروبية الجديدة، لموجب "الإبلاغ عن تسرب أو انكشاف المعلومات"، في المادة الثالثة والثلاثين منها[16]، ضمن قائمة الموجبات المفروضة، على المسؤول عن معالجة المعلومات، أو كل من تعاقد معه لتنفيذ مهمة ما، على البيانات.

في المقابل، أثبتت التقنية، عدم قدرتها على حماية ذاتها، إذ يدرك الجميع اليوم، أن ما من مؤسسة، أو منظمة، في منأى عن الاختراقات، ومخاطر انكشاف، ما لديها من بيانات شخصية، مهما كبرت، وبلغت جدية احتياطاتها الأمنية، التقنية منها، والمادية. فالتهديدات مستمرة، ومتغيرة، واللاعبون من حكومات وأفراد، لا ينفكون يتمرسون في أساليب الاختراق، والاعتداء على الأنظمة، حتى ما اعتمد منها على نظام حماية

[14] - LA BOîTE DU FUTUR [RGPD] Données personnelles : et si on arrêtait de les stocker ? 31 janvier 2018 Sachez par ailleurs que 3700 cyberattaques sont déjouées dans le monde chaque seconde (source Ciscosytem) et que 91% des fuites auraient pu être évitées… si les entreprises s’étaient dotées de mesures de sécurité suffisantes : https://blog.nextdoor.fr/2018/01/31/rgdp-donnees-perso-data-reglementation/

[15] - SECURITY BREACH NOTIFICATION LAWS
"**All** 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information".
http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[16] - Art. 33 GDPRNotification of a personal data breach to the supervisory authority
***** 1In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55

الطبقات المتعددة. فالأمن الكامل، غير ممكن، ومروحة الأضرار، التي يمكن أن تنتج عن معالجة البيانات، واستخدامها بشكل خاطئ، في اتساع متواصل.

في هذا الإطار، يمكن فهم حركات المطالبة في الولايات المتحدة الأميركية[17]، وبعض البلدان الأخرى، بتشريع مماثل للتشريع الأوروبي، ينظم حقوق الأفراد، ويعيد لهم شيئا من السيطرة على بياناتهم الشخصية. كذلك، يمكن فهم تحول الاتحاد الأوروبي، إلى مركز الثقل، في ما يتعلق بحماية الأشخاص الطبيعيين في مواجهة مخاطر معالجة البيانات، واعتماد العديد من الدول لمنهجيته[18]، التي تقوم على إقرار حقوق للأفراد، وموجبات على معالجي البيانات، والمستثمرين فيها. فإذا كانت البيانات الشخصية، محرك الاقتصاد الرقمي، والقيمة الأساسية، في السنوات القادمة، يكون من الأنسب إعطاء أصحابها، الحق في تقرير كيفية، وحدود استخدامها، من قبل مستثمريها.

وفي سعيها إلى تحقيق هذا الأمر، نلاحظ أن القواعد الأوروبية الجديدة، قد أدخلت عددا من المفاهيم الجديدة، المعتمدة في منظومة الحماية الانجلوساكسونية، والتي تعتمد في جزء أساسي منها، على حلول تقنية، يمكن أن تأخذ مكانها إلى جانب الأطر التشريعية، والتنظيمية، والتي يمكن أن تكون أضيق من استيعاب جميع الحلول الممكنة، لتأمين حماية أفضل.

البيانات الشخصية: مرتكز الخصوصية

يبدو واضحا، من التعريفات العديدة، التي اعتمدت، في القوانين التي تنظم معالجة البيانات الشخصية، أو تبادلها، أو نشرها، أن الهم الأساس من حمايتها، كما سنرى لاحقا، هو الحفاظ على حق الشخص في الخصوصية.

[17] - https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[18] - Protection des données personnelles :quand l'Europe inspire le monde
https://www.lesechos.fr/tech-medias/hightech/0301706311320-protection-des-donnees-personnelles-quand-leurope-inspire-le-monde-2178705.php

وإذا كان لا بد من التفريق، بين حماية البيانات الشخصية والحق في الخصوصية، نقول أن الخصوصية تعني، بشكل أساسي، المحافظة على السرية، ومنع التدخل، في ما يعتبر حميمية الشخص، وأسراره، عبر حماية بعض البيانات الشخصية، بشكل يمنع انتشار المعلومات التي تكشف الحياة الخاصة، أو تعرضها للانكشاف. وعليه، هنالك اعتداء على الخصوصية، سواء تعلق الأمر، بكشف سر دفين، وإيصاله إلي الآخرين، أم بمراقبة ورصد تحركات، لم يقترنا بكشف أسرار، أو بنشر معلومات حساسة. فالضرر واقع في الحالتين: إذ ينتج عن كشف المعلومات، في الحالة الأولى، وعن كون الشخص، وضع تحت المراقبة، في الحالة الثانية.

وتتمثل الجوانب القانونية، للاعتداء على الخصوصية، عبر استخدام البيانات الشخصية، بطريقة غير قانونية، في عدد من الجرائم، والأعمال غير القانونية، التي يمارسها الأفراد، أو الجهات الحكومية، ومنها: التنصت، والابتزاز، واختراق أنظمة المعلومات، والوصول إلي الأسرار المهنية والتجارية، إضافة إلى الرصد غير المشروع لحركة الأشخاص والأموال، من قبل الأجهزة الحكومية، وتكوين ملفات معلومات، دون سبب قانوني، والتمييز العنصري، والعقائدي، والديني.

من هنا، يعتبر الإقرار بحماية البيانات الشخصية، إقراراً بحق المواطن، في الحفاظ على خصوصيته، من جهة أولى، كما يعني إقراراً بحق الدولة، في الاطلاع على هذه البيانات، ومعالجتها، ضمن أطر قانونية وتنظيمية محددة وواضحة، بما يسمح للسلطات المختصة، بمنع وقوع أعمال مخلة بالأمن والنظام، أو بملاحقة ومعاقبة مرتكبيها، من جهة ثانية.

ولذلك، برز اهتمام عام، بالحفاظ على البيانات الشخصية، كخطوة ضرورية للحفاظ على الحق في الخصوصية[19]، استدعت ومنذ بداية السبعينات، اتخاذ قرارين من قبل المجلس الأوروبي، حول حماية الحياة الخاصة للأشخاص الطبيعيين، من نتائج

[19] - مؤتمر استوكهولم 1967 – مؤتمر طهران 1968 بإشراف الأمم المتحدة.

معالجتها في إطار إنشاء قواعد بيانات، في القطاعين العام والخاص، وذلك في العامين 1973 و1974.

يشكل احترام الحياة الخاصة، الأساس الذي يقوم عليه الحق في حماية البيانات ذات الطابع الشخصي، وترتبط حماية البيانات، كما هو واضح من كل ما تقدم، بالحاجة إلى حماية الحقوق والحريات الخاصة.

وفي هذا الإطار، برز اهتمام بعدد من الحقوق المرتبطة بتدفق المعلومات على الإنترنت، دون قيود، كالحق في الوصول إليها، والحق في تبادلها، ونشرها. لكن الحذر من المخاطر، التي يمكن أن تترتب على حركة المعلومات هذه، كان السبب الأساسي في إثارة مسألة الحق في الحفاظ على الخصوصية، خلال مؤتمرين عقدا بإشراف الأمم المتحدة، الأول في أستوكهولم عام 1967[20]، والثاني في إيران عام 1968. ولذلك، سنعرض لعلاقة الخصوصية بالحق في حماية البيانات الشخصية، انطلاقا من الأطر التشريعية، والنصوص الدولية، الأوروبية والعربية، قبل تناول أحكام حماية البيانات.

- **نصوص ذات علاقة**

برز الحق في الخصوصية، قبل عصر انتشار الإنترنت، من خلال حق الفرد في حماية البيئة الخاصة به، ضد أي تدخل من الآخرين، لاسيما ضد تدخل الدولة، في المادة 12 [21] من الإعلان العالمي لحقوق الإنسان، الصادر عام 1948، عن منظمة الأمم المتحدة.

[20] - http://unesdoc.unesco.org/images/0000/000025/002559eo.pdf

[21] - Article 12: Right to privacy No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
Universal Declaration of Human Rights | United Nations - K UN.ORG
www.un.org/en/universal-declaration-human-rights/

وهنا، تجدر الإشارة إلى أن جميع الدول العربية، أعضاء في الأمم المتحدة، لكن بعضها فقط، التزم هذا الإعلان، من خلال الدساتير، كقطر[22]، وموريتانيا[23]، بينما لم يرد أي ذكر لهذا الالتزام في الدستور المصري، أو التونسي. لكن هذا الأخير، أنشأ هيئة خاصة بحقوق الإنسان[24]، سميت ب "مفوضية حقوق الإنسان"، وكذلك فعل المغرب، ولكن مع إقراره التزام الاتفاقات الدولية، في مقدمة الدستور[25].

وكانت المادة الثانية عشرة، من الإعلان العالمي لحقوق الإنسان، التي نصت على احترام الحياة الخاصة، والحياة العائلية، قد أوردت استثناءات قانونية للتدخل، ترتكز بشكل أساسي، إلى ضرورات الحفاظ على امن المجتمع واستقراره، والأمن القومي، والرفاه الاقتصادي الوطني، وحريات الآخرين وحقوقهم، وحماية الصحة والآداب، على أن يكون هذا التدخل من ضمن الإطار القانوني. ويعتبر الحق في حماية البيانات الشخصية، مشمولا بهذه المادة، لان الكشف عنها، يكشف عن الحياة الخاصة.

ويعتبر هذا الإعلان، أول إطار قانوني دولي لهذا الحق. وقد أعيد التأكيد عليه، في المواد 14 إلى 17، من العهد الدولي الخاص بالحقوق المدنية والسياسية، الصادر في العام 1966، عن الجمعية العامة في الأمم المتحدة، حيث اقتبست المادة 17[26]،

---

[22] - المادة (6) من دستور قطر تحترم الدولة المواثيق والعهود الدولية، وتعمل على تنفيذ كافة الاتفاقيات والمواثيق والعهود الدولية التي تكون طرفاً فيها.

[23] - في ديباجة الدستور: اعتبارا منه لقيمه الروحية وإشعاعه الحضاري، تمسكه بالدين الإسلامي الحنيف وبمبادئ الديمقراطية الوارد تحديدها في الإعلان العالمي لحقوق الإنسان الصادر بتاريخ 10 ديسمبر 1948 والميثاق الإفريقي لحقوق الإنسان والشعوب الصادر بتاريخ 28 يونيو 1981 وفي الاتفاقيات الدولية التي وافقت عليها موريتانيا.

[24] - دستور تونس: القسم الثالث: هيئة حقوق الإنسان - الفصل 128 تراقب هيئة حقوق الإنسان احترام الحريات وحقوق الإنسان، وتعمل على تعزيزها، وتقترح ما تراه لتطوير منظومة حقوق الإنسان، وتستشار وجوبا في مشاريع القوانين المتصلة بمجال اختصاصها. تحقق الهيئة في حالات انتهاك حقوق الإنسان لتسويتها أو إحالتها على الجهات المعنية. تتكون الهيئة من أعضاء مستقلين محايدين من ذوي الكفاءة والنزاهة، يباشرون مهامهم لفترة واحدة، مدتها ستّ سنوات.

[25] - دستور المغرب....حماية منظومتي حقوق الإنسان والقانون الدولي الإنساني والنهوض بهما، والإسهام في تطويرهما ؛ مع مراعاة الطابع الكوني لتلك الحقوق، وعدم قابليتها للتجزيء؛ • القانون الدولي • المعاهدات الدولية لحقوق الإنسان • حظر ومكافحة كل أشكال التمييز، بسبب الجنس أو اللون أو المعتقد أو الثقافة أو الانتماء الاجتماعي أو الجهوي أو اللغة أو الإعاقة أو أي وضع شخصي، مهما كان؛ • ضمان عام للمساواة • المساواة بغض النظر عن الجنس • المساواة بغض النظر عن اللون • المساواة بغض النظر عن العقيدة أو المعتقد • المساواة بغض النظر عن بلد المنشأ • المساواة بغض النظر عن اللغة • المساواة لذوي الإعاقات • جعل الاتفاقيات الدولية، كما صادق عليها المغرب، وفي نطاق أحكام الدستور، وقوانين المملكة، وهويتها الوطنية الراسخة، تسمو، فور نشرها، على القوانين الوطنية، والعمل على ملاءمة هذه • القانون الدولي القوانين، مع ما تتطلبه تلك المصادقة.

[26] - Article 17 - 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.
http://www.claiminghumanrights.org/privacy_definition.html

أحكام المادة 12، وأضافت مفهوم عدم الشرعية، على الاعتداء، والتدخل، اللذين يطالان هذا الحق.

كما كان لهذا الإعلان، أثر أكيد في الإعلان الخاص بحقوق الإنسان في أوروبا[27]، الصادر في العام 1950، والذي نص في المادة الثامنة منه على احترام الحياة العائلية للأفراد، كأحد الحقوق الأساسية للإنسان.

وفي العام 1959، أنشئت المحكمة الأوروبية لحقوق الإنسان، لمتابعة تنفيذ هذا الإعلان، والتزام الدول الأعضاء بمندرجاته، وذلك، عبر النظر في مراجعات الأفراد، أو المجموعات، أو الجمعيات، أو الأشخاص المعنويين، ضد ما يمكن أن يشكل انتهاكا لحقوق الإنسان، التي أقرت في الاتفاقية.

ويمكن لهذه المحكمة، النظر في قضايا ترفع من قبل دولة، أو عدد من الدول الأعضاء، ضد دولة أخرى، عضو في الاتحاد الأوروبي، انتهكت هذا الإعلان.

وبالفعل، فقد نظرت المحكمة، في العديد من القضايا، استنادا إلى هذه المادة، لاسيما منها قضايا الرقابة، وحفظ البيانات الشخصية. وقد أكدت، في القرارات ذات الصلة، على موجب الدولة، ليس فقط في الامتناع عن التدخل في الحياة الخاصة للأفراد، دون سند قانوني، وإنما أيضاً، على واجبها في اتخاذ الإجراءات، التي تضمن حماية هذه الخصوصية.

وقد لعب الدليل حول حماية الخصوصية، والذي أصدرته منظمة التعاون الاقتصادي والتنمية، دورا أساسيا، في التوجهات التشريعية للدول الأوروبية، التي تبنت مبادئه، وهي: محدودية عمليات جمع البيانات Collection-limitation، نوعية

[27] - ARTICLE 8 Right to respect for private and family life 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
https://www.echr.coe.int/Documents/Convention_ENG.pdf

البيانات Data quality، تحديد الهدف Purpose-specification، حصر الاستخدام بالهدف المحدد Use-limitation، تأمين وسائل حماية وامن المعلومات Security-Safeguards، العلانية Openness، والحق في المشاركة والمساءلة Individual Participation and Accountability. علما أن هذا الدليل، قد استهدف حماية البيانات الخاصة بالأشخاص الطبيعيين، المعالجة آليا، أو يدويا، في القطاعين العام والخاص.

وكانت الأمم المتحدة، قد تبنت في العام 1990، من خلال هيئتها العامة، دليلا لتنظيم المعالجة الآلية للبيانات الشخصية، تضمن مبادئ الدليل، الذي أصدرته منظمة التعاون الاقتصادي والتنمية.

على المستوى العربي، أقرت بعض الدول العربية، حماية الحياة الخاصة، من خلال نص دستوري، كما فعلت مصر في المادة 45 من الدستور[28]، بإقرارها حماية الحياة الخاصة للمواطنين، وتجريمها كل اعتداء عليها، في المادة 57، وقطر في المادة 37[29]، والذي أقر حرمة خصوصية الإنسان. أما الدستور التونسي، الذي أقر الحق في الخصوصية[30]، في المادة 24 منه، فقد تفرد بتحديد المعطيات الشخصية، كواحد من العناصر التي يجب الحفاظ على سريتها، في إطار المحافظة على الحياة الخاصة، إلى جانب حرمة المسكن، وسرية المراسلات، والاتصالات. أما المغرب، فقد ركز إلى جانب حماية الحق في حماية الخاصة، على حماية الاتصالات.[31]

---

[28] - دستور مصر: مادة(45): لحياة المواطنين الخاصة حرمة يحميها القانون.
وللمراسلات البريدية والبرقية والمحادثات التليفونية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة، ولا تجوز مصادرتها أو الإطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة ووفقا لأحكام القانون.
مادة(57): كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتكفل الدولة تعويضا عادلا لمن وقع عليه الاعتداء.
تونس: الفصل 24 الحق في احترام الخصوصية

[29] - دستور قطر : المادة 37
لخصوصية الإنسان حرمتها، فلا يجوز تعرض أي شخص، لأي تدخل في خصوصياته أو شؤون أسرته أو مسكنه أو مراسلاته أو أية تدخلات تمس شرفه أو سمعته، إلا وفقا لأحكام القانون وبالكيفية المنصوص عليها فيه.

[30] - الدستور التونسي لعام 2014 : "تحمي الدولة الحياة الخاصة، وحرمة المسكن، وسرية المراسلات والاتصالات والمعطيات الشخصية".

[31] - دستور المغرب: الفصل 24 • الحق في احترام الخصوصية لكل شخص الحق في حماية حياته الخاصة. لا تنتهك حرمة المنزل. ولا يمكن القيام بأي تفتيش إلا وفق الشروط والإجراءات التي ينص عليها القانون. لا تنتهك سرية الاتصالات الشخصية، كيفما كان شكلها. ولا يمكن الترخيص بالاطلاع على مضمونها أو نشرها، كلا أو بعضا، أو باستعمالها ضد أي كان، إلا بأمر قضائي، ووفق الشروط والكيفيات التي ينص عليها القانون

وكذلك فعل الدستور الجزائري في المادة 46 منه، والمادة 39، حين حرم انتهاك حرمة حياة المواطن الخاصة، واعتبر حماية البيانات الشخصية، العائدة للأشخاص الطبيعيين، حقا أساسيا، يعاقب القانون على انتهاكه. ونص الدستور الليبي، في المادة 16 منه، على أن: للحياة الخاصة حرمة، ويحظر التدخل فيها، إلا إذا شكلت مساسا بالنظام والآداب العامة، أو إضراراً بالآخرين، وإذا اشتكى أحد أطرافها. ونص الدستور الموريتاني، في المادة 13، انه على الدولة، أن تضمن شرف المواطن، وحياته الخاصة.

إلى ذلك، يمكن إضافة بعض الدساتير، التي نصت على ما يمكن اعتباره، حماية لمكون من مكونات الخصوصية: حرية الاتصالات وسريتها. وقد أوردت ذلك، دساتير اليمن في المادة 52، وسلطنة عمان في المادة 30، والصومال في المادة 22.

أما في لبنان، فتتوزع الأحكام ذات العلاقة، على الدستور من جهة، وبعض القوانين الوضعية، من جهة ثانية. لذا يمكن القول، أن الأساس لحماية البيانات الشخصية، في لبنان، هو دستوري، وغير مباشر. فالدستور اللبناني، يعلن في مقدمته، عن التزام الشرع الدولية والاتفاقات العالمية الخاصة بحقوق الإنسان، وذلك دون أي تمييز بين أبناءه. كما يعتبر احترام الحريات العامة والحقوق، من ركائز الجمهورية الديمقراطية البرلمانية، وفي مقدمها، حرية المعتقد والرأي، والعدالة الاجتماعية والمساواة.

ويبدو واضحا أن الدستور اللبناني، على غرار العديد من الدساتير، التي سبقت تقنيات المعلومات والاتصالات، حول العالم، يتعامل مع الخصوصية ببعدها المادي، من خلال إقراره حرمة المنزل، والحرية الشخصية، واحترام الملكية. ألا انه يتعامل معها أيضا ببعدها غير المادي، عندما يقر حرية الرأي والمعتقد، وحرية التعبير عن الرأي. علما انه يضع حدودا لهذه الحريات، هي النظام العام والآداب، واحترام

حقوق الآخرين. وقد أقرت المادة الثامنة منه، وعلى غرار مجمل الدساتير العربية، مبدأين أساسيين في حماية الحريات والحقوق هما: مبدأ شرعية الجرائم والعقوبات، والثاني مبدأ إخضاع الإجراءات التي تمس الحقوق والحريات، إلى القانون.

ويعزز الاحتكام إلى القانون وسلطته، مبادئ أخرى، مثل مبدا دستورية القوانين، والفصل بين السلطات. وعليه، يصبح تدخل السلطة في الحياة الخاصة للأفراد ممكنًا، عندما تسمح بذلك النصوص القانونية، بهدف حماية الأمن القومي، والمصلحة العامة، والنظام الاجتماعي، والاقتصادي، والأخلاقي، والصحة العامة والآداب. ويمثل ذلك، على مستوى البيانات الشخصية، إقرارا بحق الدولة في الاطلاع عليها، ومعالجتها، بما يسمح للسلطات المختصة، بمنع وقوع أعمال مخلة بالأمن والنظام، أو بملاحقة ومعاقبة مرتكبيها.

- **تعاظم المخاطر**

تقر أنظمة الحكم، في مختلف البلدان، لاسيما منها تلك التي تعتمد النظام الديمقراطي، وتلتزم شرع حقوق الإنسان، مجموعة من الأحكام التشريعية والتنظيمية، والقواعد الإجرائية والقضائية، تسمح بتحقيق الأمن والاستقرار في المجتمع، وبتأطير حماية الحريات الفردية، وحقوق الإنسان، بحيث لا تتعرض للاعتداء من قبل السلطات المسؤولة.

إلا أن تعاظم مستوى المخاطر، التي تتعرض لها المجتمعات المختلفة، نتيجة اعتمادها المتزايد على بنية تحتية ترتكز بشكل أساسي، إلى تكنولوجيا المعلومات والاتصالات، وتصاعد مستوى حركة تبادل المعلومات، من جهة أولى، إضافة إلى بروز مخاطر الجرائم السيبرانية، التي تتجاوز الحدود الجغرافية لمختلف البلدان، وتهدّد البنية التحتية للاتصالات، من جهة ثانية، زاد من قلق الحكومات، والأجهزة الأمنية، وجعلها تتجه نحو مراقبة مستخدمي الإنترنت، كوسيلة من وسائل رصد الأفراد ومراقبتهم،

انطلاقا من كونها المعنية بالحفاظ على السلامة العامة، والأمن، بكل أشكاله. مما جعل المخاوف تتصاعد، من احتمالات الاعتداء على الحق في الخصوصية، وما يرتبط به من حقوق إنسانية، وحريات مدنية.

فقد ترافق دفق الكميات الهائلة من البيانات الشخصية، على الإنترنت، وفي الفضاء السيبيري، مع تقنيات جد متطورة، ومنهجيات معالجة، يمكنها أن تشكل تهديدا مباشرا، ليس فقط للأشخاص الذين تساعد في كشف هوياتهم، وإنما أيضاً للدول، ولمصالحها الحيوية، وأمنها. ويتمثل هذا التهديد، في الاعتداءات التي يمكن أن تقع على الأشخاص، الطبيعيين والمعنويين، في القطاعين العام والخاص، وعلى البيانات والمعلومات؛ سواء من خلال سرقتها، أو تعديلها دون وجه حق، أو تشويهها، وفي الاعتداءات على أنظمة المعلومات، ومنع عملها، وعلى الحريات والحقوق التي يتمتع بها الأفراد، في المجتمعات الديمقراطية، كالحق في الخصوصية، والحق في التعبير.

فلقد وفرت تقنيات المعلومات والاتصالات، والأجهزة التي تستخدمها، قدرة هائلة، وإمكانات غير مسبوقة، على مستوى حفظ البيانات، ومعالجتها، كما ونوعا، ما خلق حركة نوعية، تستند إلى تقدم التقنيات، وتشعب الإمكانات التي تتيحها، في مجال الجمع، والتنقيب عن البيانات، وتحويلها إلى معلومات، حول كل ما ومن يتصل، أو لا يتصل، بالإنترنت.

إلا أن هذه الآفاق والفرص الجديدة، حملت معها تهديدات، ومخاطر، طرحت تحديات على مستوى حماية الحقوق والحريات، التي يمكن أن تتأثر، نتيجة جمع البيانات، أوجمعها، بطريقة عشوائية، غير منظمة، وخارج الأطر القانونية الملائمة، أو نتيجة لانكشاف البيانات التي تمت معالجتها، ووقوعها، بين أيدي الأشخاص غير المناسبين.

فتصاعد القلق من الجرائم، التي يمكن أن تنتج، عن انكشاف البيانات الشخصية، لاسيما منها، تلك التي تستهدف الأشخاص، في سمعتهم، أو عبر تهديدهم، وابتزازهم، والتحرش بهم، والانتقام الجنسي منهم، أو التنمر، نتيجة جمع أو تسرب بياناتهم الشخصية، كمحادثاتهم، ورسائلهم، وصورهم الحميمة.

وقد كشفت إحدى الدراسات، التي أجريت في العام [32]2016، عن تعرض 47% من مستخدمي الإنترنت في أميركا، لنوع من التحرش الجنسي، وأن 5% منهم، على الأقل، تعرضوا للأذى، نتيجة تسرب بياناتهم الحساسة.

في المقابل، تأكدت حقيقة الخطر الأدهى، الكامن في جهل غالبية مستخدمي الإنترنت، لحقوقهم، ولحقيقة جمع بياناتهم ومعالجتها، ونشرها، واستخدامها[33].

وكانت مساءلة مارك زوكربيرغ، مالك فيسبوك، عن فضيحة استثمار البيانات الشخصية لمستخدمي الموقع[34]، ونقلها إلى جهات ثالثة، قد أثارت انتباه العالم مجددا، حول خطورة الاعتداءات على حقوق مستخدمي الإنترنت، ومدى اجتياحها للحياة الخاصة وحقوق الإنسان، لاسيما عندما يتم جمع هذه البيانات، دون علم صاحبها، ودون موافقة صريحة منه. هذا عدا عن إضاءتها، على التهديدات التي يشكلها قطاع الإعلانات الرقمية[35]، على الحياة الخاصة، لاسيما عندما يلجأ إلى أساليب تحليل البيانات، ودراسة تقاطعها، لمعرفة علاقات صاحبها، واهتماماته،

---

[32] - http://time.com/4579785/internet-users-harassment-study/
Almost Half of U.S. Internet Users Have Experienced Online Harassment - The types of harassment were divided into three categories: digital harassment (e.g. being called offensive names), invasion of privacy (e.g. being hacked or impersonated) and denial of access (e.g. technical attacks that overwhelm a device, site, server or platform and prevent access).

[33] - https://www.kau.se/en/cs Few keep track of their personal data on online

[34] - The key moments from Mark Zuckerberg's testimony to Congress
https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments
- This is how Facebook uses your data for ad targeting
https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg

[35] - Facebook's data breach scandal is making headlines and this psychologist is at the centre of it all
//economictimes.indiatimes.com/articleshow/63382398.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
https://economictimes.indiatimes.com/magazines/panache/facebooks-data-breach-scandal-is-making-headlines-and-this-psychologist-is-at-the-centre-of-it-all/articleshow/63382398.cms

وتحديد ما يمكن أن يثير اهتمامه من خدمات، و منتجات وبضائع، ومعلومات.

وتصبح الأمور مقلقة اكثر، فيما لو نظرنا إلى حجم البيانات، التي يجمعها محرك البحث غوغل، ومدى متابعته حركة المبحرين على الإنترنت، وتسجيل الوقت الذي يمضونه على المواقع المختلفة، وفي استخدام التطبيقات، وبعض المنصات الرقمية.

وفي هذا السياق، يلاحظ تتابع فضائح تسرب البيانات الشخصية على الإنترنت[36]، منذ بدء استخدام تقنيات المعلومات والاتصالات لجمعها، ومعالجتها. وتزداد فداحة تأثير هذا التسرب، مع تطور قدرات تقنيات المعلومات والاتصالات، وازدياد حجم البيانات الشخصية، والإقرار بتحولها إلى قطاع نفط جديد، ومحور حيوي لعدد من النشاطات، الحكومية والتجارية كذلك، تتابع أخبار استخدام الدول عامة[37]، والعربية[38] منها خاصة، لبرامج وتطبيقات الرصد والرقابة على الإنترنت، وعلى الهواتف الذكية، وغيرها من الأجهزة المتصلة بالإنترنت. وعليه، كان لا بد من التحرك، لمواجهة هذه التحديات.

وتصبح هذه التهديدات، أشد خطورة، ويتعاظم الخوف من الاعتداء على البيانات الشخصية، عندما يتعلق الأمر بالتزام الدول، مكافحة بعض الأعمال والجرائم، ذات الارتدادات الكارثية: كالإرهاب مثلا، حيث تستعمل البيانات الشخصية، بشكل منهجي، من قبل الحكومات المختلفة، سواء في أنشطتها الوطنية الداخلية، أو في علاقاتها مع الدول الأخرى، من خلال اتفاقيات[39]، أو من خلال أنظمة

[36] - Small business data breaches reach all-time high - Written on Mar 14, 2018
https://www.ohiocpa.com/search/utilities/displaynewsitem/2018/03/14/small-business-data-breaches-reach-all-time-high
- Data breaches reach all-time high as new environments create more attack surfaces 7 February 2018 | Author: Sunetra Chakravarti
https://teiss.co.uk/threats/data-breaches-reach-time-high-new-environments-create-attack-surfaces/

[37] - China's Surveillance State Should Scare Everyone - The country is perfecting a vast network of digital espionage as a means of social control—with implications for democracies worldwide
https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

[38] - Dark Caracal: Global Espionage Malware from Lebanon
https://www.schneier.com/blog/archives/2018/01/dark_caracal_gl.html

[39] - Les accords entre l'union européenne et les états unis. * le traite de prum, signe le 27 Mai 2005

أمن، وبرامج متخصصة[40].

في هذا السياق، تثير حماية البيانات الشخصية، عددا من الإشكاليات، نتيجة التقائها أو تناقضها، مع عدد من الحقوق والحريات الأخرى، مثل: التدفق الحر للمعلومات، والحق في الوصول إلى المعلومة، وحق الدولة في الرقابة على القيود الخاصة بالمواطنين، وحقها في ضبط هذه القيود، وغيرها.

وعليه، تترك إدارة البيانات، في القطاعين العام والخاص، اثرها، بشكل واضح على المجتمع، حيث تطرح، تحديات أمام الحكومة والمشترع، وواضعي سياسات الحماية، ومصنعي البرامج، من خلال الهواجس، التي تثيرها مسائل الحفاظ على الحق في الخصوصية، وأمن البيانات، وأساليب جمعها، ومعالجتها، ومصداقيتها.

مصادر الخطر

تعود مصادر الخطر، على الحق في الخصوصية، إلى طبيعة التقنية، من جهة أولى، وغياب الأطر التشريعية والتنظيمية الملائمة، من جهة ثانية، وقصور نماذج الحماية التقليدية، من جهة ثالثة. في هذا الإطار، يمكن الإشارة إلى عدد من الاعتبارات، التي تتوزع عمليا، على القطاعين العام والخاص، وعلى الأفراد، والأشخاص المعنويين.

- اعتبارات تقنية - اقتصادية - اجتماعية - سياسية

بالرغم من الاعتراف به، من قبل العديد من الدول والشرع والقوانين[41]، يبقى الحق في الخصوصية، وتبقى البيانات الشخصية، عرضة للاعتداء، ليس فقط نتيجة

---

[40] - les systèmes d'échanges d'informations crées a l'échelle de l'Union Européenne : le système d'information Schengen (SIS), le système d'information douanier, et le système d'information d'Europol et celui d'Eurojust.

[41] 47 - الحق في الخصوصية من الحقوق الأساسية، المعترف بها في عدد من البلاد حول العالم، وفي نصوص عالمية، مثل الدساتير الوطنية والاتفاقية. الإعلان العالمي لحقوق الإنسان، شرعة الحقوق السياسية والمدنية، الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات، والاتفاقية الأميركية لحقوق الإنسان.

The Universal Declaration of Human Rights,(Article 17) of the International Covenant on Civil and Political Rights, (Article 8) of the European Convention on Human Rights, (Article 11) of the American Convention on Human Rights.

Article 12 of the Universal Declaration of Human Rights states, "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."

النقص التشريعي والتنظيمي، والممارسات الحكومية، وإنما نتيجة للإمكانات التقنية الهائلة، التي تتيحها تقنيات المعلومات والاتصالات، والتي لا يمكن توقع مداها ولا قدرتها. ونذكر هنا على سبيل المثال: تقنيات الرصد، وجمع البيانات، والتتبع، والمعالجة، والتنقيب، والوصول بسرعة فائقة، إلى عدد أكبر من الناس، في أماكن مختلفة من العالم.

يضاف إلى ذلك، استحالة معالجة النتائج السلبية للاعتداءات، في أحيان كثيرة، مع تعذر استعادة البيانات التي تم الاستيلاء عليها، أو تعذر عملية السحب، أو الإلغاء الكامل للبيانات أو الأخبار، التي تم نشرها، أو تشويهها، أو تزويرها والتلاعب بها. يضاف إلى ذلك، الخطر الذي يمثله، اقتحام بعض قواعد المعلومات الشخصية، سواء منها تلك التي تحتفظ بها الشركات، أو تلك التي تحتفظ بها الجهات الرسمية[42].

وقد اثبت انتشار الشبكات الاجتماعية على الإنترنت، الحجم الكبير الذي يمكن أن تتخذه الأبعاد الاجتماعية والسياسية، لاستخدام هذه التقنيات، لاسيما على مستوى مخاطر تلاشي الخصوصية.

فمما لا شك فيه، أن هذه الشبكات قد عززت نزعة عرض الذات، بشكل مفرط، نتيجة تصميمها، وهندسة خدماتها، بطريقة تشجع على هذا الاستعراض، وعلى بث كل تفاصيل الحياة الخاصة. وكلما ازداد عدد مستخدمي موقع ما، كلما ازدادت قدرته على جذب عدد اكبر منهم. لذلك، تعتمد التطبيقات، والشبكات الاجتماعية المختلفة، سياسة استقطاب، تقوم على تقديم عضوية مجانية، لمستخدمي الإنترنت، ما يسمح لها، بتغطية الكلفة المرتفعة للتمويل، والتي تعتبر أساسية في إدارتها وتطويرها، عبر الاستثمار في الإعلانات.

[42] - منى الأشقر جبور ومحمود جبور- القانون والإنترنت: تحدي التكيف والضبط- المنشورات الحقوقية- صادر- بيروت- 2008

ولهذا السبب، تتخذ الشبكات الاجتماعية، أحيانا كثيرة، طابع شركات الإعلان، التي تستخدم البيانات الشخصية، لجذب أموال المعلنين، بناء على تصنيف أوتوماتيكي، يتم بعالجة بيانات الشخص المعني، بطريقة تظهر اهتماماته، واحتمالات تجاوبه مع إعلان عن خدمة ما، أو منتج ما.

فشركة فيسبوك مثلا، تجمع كل البيانات الخاصة بمستخدميها، والتي تتيح لها معرفة أدق التفاصيل، عن حياتهم الشخصية، وميولهم. وهي لئن كانت لا تبيع هذه البيانات، إلا إنها تبيع حق الوصول اليهم، لشركات الإعلانات.

ولو توقفنا عند الأسئلة، التي يطرحها الفيسبوك على مستخدميه، ماذا في ذهنك الآن؟ ما الجديد اليوم؟ وغيرها، يمكننا التأكد أن الأمر يتجاوز الاهتمام، بتأمين منصة تبادل أخبار بين الأصدقاء، ونقاش حول قضايا معينة، إلى سعي دؤوب لفهم ميول المستخدم، ورصد تفاصيل حياته اليومية، بحيث يصبح من السهل رسم طيف خاص به، وتحديد كيفية استهدافه، بالإعلانات، أو الأخبار، أو الانضمام إلى مجموعات تبحث عن مؤيدين، ومتابعين.

وهكذا تبرز شبكات التواصل الاجتماعي، كشكل جديد من أشكال التحكم الاجتماعي، حيث يمكن لأي كان، مراقبة نشاط، وتحركات، شخص آخر. وتتم هذه الرقابة، على مستويين، الأول مرئي، ويقوم به الأصدقاء، أو متتبعو نشاط الشخص المعني، والثاني، وهو غير مرئي، وتقوم به البرامج، والتطبيقات، المتخصصة في رصد وتحليل الاهتمامات، والشخصية، والتي تستخدمها المواقع المختلفة، ومحركات البحث.

ويضاف إلى ذلك، اهتمام قطاع تطوير البرامج، والشركات المعلوماتية الكبرى، التي تسعى إلى فهم مدى حرص مستخدم الإنترنت على خصوصيته، بحيث تتمكن

من استشراف تقنيات الحماية، التي تحسن قدرتها التنافسية[43]. كما يمكن لهذه الشركات، أن تستثمر، في برامج اختراق الخصوصية، وكسر طبقات الحماية، من خلال بيع "أنظمة وبرامج اختراق"، لبعض الدول، التي تمارس رقابة شاملة على مواطنيها.

وهذا ما يجعل الحدود بين الفرد والمجتمع، تتلاشى، بفعل إرادي من المستخدم، الذي ينشر بياناته، الأمر الذي بات يستدعي، إعادة النظر، في تحديد مضمون الحق في الخصوصية. ويشكل هذا الأمر الأخير، واحدا من التحديات، التي تستدعي تدخل المشترع، للحفاظ على حق من الحقوق الأساسية للإنسان.

فالبيانات الشخصية، كما ذكرنا، قيمة اقتصادية، يسعى إليها المستثمرون بكل الوسائل، من أجل تعزيز فرص وصولهم إلى شرائح أكبر وأوسع من الزبائن، وإلى تنمية فرص استثماراتهم، عبر تحديد أطياف، وسمات الأشخاص. لكنها أيضا، قيمة مرتبطة بحق إنساني، وبإمكانية ممارسة العديد من الحريات. لذلك، نلاحظ الارتباط الوثيق، بين بناء الثقة، وحماية البيانات الشخصية، كواحدة من الخطوات الأساسية، التي لا بد من اتخاذها، في إطار حماية النمو الاقتصادي، سواء منه التقليدي، أم الرقمي.

وكانت المادة الرابعة، من قانون حماية البيانات الإماراتي، قد أظهرت الوجه الاقتصادي، والاجتماعي، والتنموي لقانون حماية البيانات الشخصية، حين حددت أهداف القانون بتمكين الإمارة من تحقيق رؤيتها في جعل دبي مدينة ذكية، وإدارة بيانات دبي وفق منهجية واضحة ومحددة، تتفق مع أفضل الممارسات العالمية، وتحقيق التكامل والتناغم بين الخدمات التي تقدمها الجهات الحكومية الاتحادية، والجهات الحكومية المحلية، والإفادة المثلى من البيانات المتوفرة، لدى مزودي البيانات، هذا، إضافة إلى تعزيز الشفافية، وإرساء قواعد الحوكمة بشأن

---

[43] - What Is Privacy Worth? Alessandro Acquisti, Leslie K. John, and George Loewenstein
https://www.hbs.edu/faculty/Publication%20Files/AcquistiJohnLoewenstein13_334936de-38a8-4d99-b90c-c3c02dae48b2.pdf

نشر وتبادل البيانات، وزيادة كفاءة الخدمات، التي تقدمها الجهات الحكومية الاتحادية، والجهات الحكومية المحلية للمتعاملين، من حيث مستوى الجودة وسرعة الإنجاز، وتبسيط الإجراءات، وتخفيض كلف التشغيل.

ويهدف القانون كذلك، إلى زيادة القدرة التنافسية لمزودي البيانات، ورفع مؤشر تنافسية الإمارات على المستوى الدولي، ودعم عملية اتخاذ القرار لدى الجهات الحكومية الاتحادية، والجهات الحكومية المحلية، وتمكينها من إعداد سياساتها، وتنفيذ خططها ومبادراتها الاستراتيجية بكفاءة وفعالية. وكذلك، ترسيخ ثقافة الإبداع، والإسهام في دعم المبادرات الابتكارية، التي من شأنها تحقيق رفاهية العيش ومقومات النجاح في المجتمع، وتحقيق التوازن بين عملية نشر وتبادل البيانات، والحفاظ على سريتها وخصوصيتها، علاوة على توفير البيانات اللازمة للجهات غير الحكومية، بهدف دعم الخطط التنموية والاقتصادية في الإمارة.

ولفهم عمق تداخل الاعتبارات الأمنية، والسياسية، والاقتصادية، على مستوى حماية البيانات، والحق في الخصوصية، لا بد من إلقاء نظرة على ما يحصل من تعاون بين الدول، على مستوى الرقابة. ففي تقرير، أصدرته منظمة، "الخصوصية العالمية"، ظهرت ضخامة المبالغ، التي تستثمر، لنقل خبرات الرقابة، وتقنياتها، من الدول المتقدمة، إلى الدول الأقل تقدما، حول العالم[44]، وبلغت النسبة التي خصصت لتدريب أجهزة، وإدارات هذه الدول، 35%، من إجمالي نفقات المعونة الخارجية الأميركية، العسكرية وغير العسكرية.

ويتضح من التقرير، تصاعد قيمة، ما ينفق في هذا المجال، بشكل لافت[45]. على

[44] - Tuesday, July 17, 2018
Countries with powerful security agencies are spending literally billions to equip, finance and train security and surveillance agencies around the world — including authoritarian regimes. This is resulting in entrenched authoritarianism, further facilitation of abuse against people, and diversion of resources from long-term development programmes.
https://privacyinternational.org/report/2159/teach-em-phish-state-sponsors-surveillance

[45] - In 2001, the US spent $5.7 billion in security aid; in 2017 it spent over $20 billion.

مستوى متصل، تتعاون، إدارات العدل، والدفاع، في الولايات المتحدة الأميركية، على تسهيل قدرات المراقبة في الدول الأجنبية، حيث تستفيد شركات الأسلحة الكبيرة، من هذه البرامج وتدمجها فيها، كما تدمجها في قواعد تدريب المراقبة في الولايات المتحدة. علاوة على ذلك، تقدم هذه الوكالات، برامج اعتراض الاتصالات، وتقنيات المراقبة الأخرى، كما تمول برامج التنصت على المكالمات الهاتفية، وتدرب وكالات التجسس الأجنبية، على تقنيات المراقبة في جميع أنحاء العالم[46].

وهنا يمكننا استشفاف خطر، الرقابة على الحكومات، الذي يتأتى عن الممارسات المذكورة.

- **ممارسات السلطة العامة**

غالبا، ما تستخدم السلطة البيانات الشخصية، وتنقلها، وتتبادلها، تحت شعار الدفاع عن الأمن القومي، أو نتيجة التزام الدول، مكافحة بعض الأعمال والجرائم ذات الارتدادات الكارثية: كالإرهاب مثلا. وفي هذا المجال، تستعمل البيانات الشخصية بشكل منهجي، من قبل الحكومات المختلفة، سواء في أنشطتها الوطنية الداخلية، أو في علاقاتها مع الدول الأخرى، سواء من خلال اتفاقيات[47]، أو من خلال أنظمة أمن وبرامج متخصصة[48]، كتلك الخاصة بإدارة شؤون إعطاء تأشيرات السفر، أو بتبادل بيانات المسافرين.

ولأن مصادر الخطر على الخصوصية، تكمن في الاستخدام غير القانوني للبيانات الشخصية، أي دون اعتبار لحقوق أصحابها، لاسيما حقهم في الخصوصية، كان لا بد من رسم حدود واضحة، لا يمكن للدولة أن تتجاوزها، منعا للاعتداء على

[46] - In 2015, military and non-military security assistance in the US amounted to an estimated 35% of its entire foreign aid expenditure

[47] - Les accords entre l'union européenne et les états unis.
* Le traite de prum, signe le 27 Mai 2005

[48] - Les systèmes d'échanges d'informations crées a l'échelle de l'Union Européenne : le système d'information Schengen (SIS), le système d'information douanier, et le système d'information d'Europol et celui d'Eurojust.

الحريات والحقوق، الأمر الذي يمكن أن يحصل، من خلال نصوص قانونية تمنح الحكومة صلاحيات واسعة، دون رقابة عليها.

» الأمن القومي

والمثال، الذي يمكن تقديمه هنا، هو القوانين[49] التي وضعت في العديد من الدول، بعد اعتداءات الحادي عشر من أيلول 2001، تحت عنوان مكافحة الإرهاب. فقد أقرت في الولايات المتحدة الأميركية، مثلا، صلاحيات واسعة للحكومة، وأعطيت أجهزتها الأمنية، حرية أكبر على مستوى التحقيق. كذلك، استبعدت المسؤولية عن أشخاص القانون الخاص، في حال إفشاءهم معلومات للحكومة، ما يمكن ترجمته عمليا، بتسليم الجهات الحكومية، البيانات الشخصية العائدة لزبائن الشركات، أو لمستخدمي شبكات التواصل الاجتماعي، وتطبيقات الاتصال المختلفة.

وانطبعت السنوات التي تلت أحداث الحادي عشر من أيلول الإرهابية، بتصاعد حركة إنشاء السجلات الحكومية، وجمع البيانات الشخصية، في خطوة اتسمت بالهم الأمني، ومواجهة الإرهاب. وكان من الطبيعي، أن تظهر بعض الممارسات والقوانين، التي تميل إلى ترجيح كفة الأمن، على كفة مصالح الأفراد، لاسيما منها، تلك المتعلقة بتأمين حماية الحياة الخاصة، والحريات.

وترافق ذلك، مع تقديم الشركات العاملة في مجال الإنترنت، خدمات مجانية لمستخدميها، مقابل الحصول على بياناتهم الشخصية، ما يدفع إلى التفكير، بان "الحياة الخاصة"، أو الحق في الخصوصية، هو ما يقدمه الشخص المعني، كثمن لحصوله على الخدمة، إذا افترضنا، بان العقد هو شرعة المتعاقدين.

---

[49] - Le Patriotact aux états unis. - Plan d'action contre le terrorisme adopte par le parlement européen et modifie le 25 Mars 2004 suite aux attentats de Madrid puis suite aux attentats de Londres du 7 juillet 2005 - recommandation relative a l'élaboration de «profiles terroristes» adoptée par le conseil européen en 2002 - directive du 15 Mars 2006 qui a prévu la conservation des données téléphoniques par les operateurs.

وهنا، يفترض الرجوع إلى شروط العقد الصحيح، وصحة الإرادة، وقدرة التمييز لدى المتعاقد. فهل توقف هذا الأخير عند تأثير موافقته هذه، وهل أدرك فعلا مدى انعكاسها، على حق أساسي تقره له الشرع الدولية، وهل كان له فعلا حق الخيار، أو رفض الموافقة؟

في هذا السياق، أعرب البرلمان الأوروبي عن قلقه، إزاء الأثر الذي يمكن أن تتركه، إجراءات تستهدف تحقيق الأمن، على الحقوق والحريات، حيث أبدى تخوفه، من أن يؤدي التعاون الدولي في مكافحة الإرهاب، إلى التخفيف من مستوى حماية الحريات، والحقوق الأساسية للإنسان، لاسيما منها حماية الحق في الخصوصية، وحماية البيانات الشخصية، وعدم التمييز[50].

وكانت التوصية الأوروبية الصادرة في العام [51]2002، قد حددت الأمن القومي، بأنه:"أمن الدولة، والدفاع، والسلامة العامة". وعليه، فالأمن القومي هو جميع الإجراءات القانونية، والإدارية، والعسكرية والأمنية، التي تهدف إلى حماية بلد معين، ضد أي نوع من التهديدات والأخطار، التي يمكن أن تعرض سلامة مواطنيه، و أراضيه، وسيادته، ورفاه المجتمع.

لكن مفهوم الأمن القومي، شهد توسعا في العصر الحالي، فأصبح يشمل السلامة المادية للشخص، أو الوطن، إلى جانب الأمن الاقتصادي، والأمن الاجتماعي، والأمن الإنساني. وهكذا، بتنا نشهد تنسيقا متزايدا، بين إدارات الأمن والاقتصاد[52]، وربطا، بين أمن الفضاء السيبيري، والاقتصاد، والأمن

[50] - Résolution du 14 janvier 2009 sur la situation des droits fondamentaux dans l'Union européenne (2004-2008).le Parlement européen « se préoccupe du fait que la coopération internationale dans la lutte contre le terrorisme a souvent abouti à une baisse du niveau de protection des droits de l'Homme et des libertés fondamentales,notamment du droit fondamental au respect de la vie privée, à la protection des données à caractère personnel et à la non-discrimination

[51] - La directive européenne 2002/58/CE, remplacée par la directive 2006/24/CE. La sécurité nationale est "… la sûreté de l'état, la défense, et la sécurité publique…"

[52] - L'institution militaire en France loge, le poste de Haut représentant charge de l'intelligence économique (HRIE), responsable de la coordination des réponses gouvernementales en ce domaine, a savoir le secrétariat général de la défense nationale (SGDN).

القومي، في خطابات العديد من قادة العالم.

فقد أعلن الرئيسي الأميركي، باراك اوباما، أن امن الفضاء السيبيري، يأتي في مقدمة اهتماماته، معتبرا التهديد الآتي منه، من أخطر المسائل، التي تطرح على المستوى الاقتصادي، كما على مستوى الأمن القومي، ما دفعه إلى تعيين مسؤول عن أمن الفضاء السيبيري، يكون على اتصال وتنسيق دائمين معه، ويكون عضوا في الأمن القومي، وفي المجلس الاقتصادي الوطني[53]. ولم تتأخر الإدارة الأميركية، عن استحداث قيادة عسكرية جديدة، تتولى أمن الفضاء السيبيري[54].

وكان رئيس الوزراء الإنكليزي، غوردن براون، قد اعلن هو أيضاً، عن إنشاء وحدة خاصة، لمكافحة الجريمة السيبيرانية[55]. إلا أن الرئيس الأميركي، حرص في المقابل، على تأكيد التزام إدارته، بحرية الإنترنت، وبحرية الاتصالات، معتبرا أن من واجبها، حماية الحريات المدنية، والحق في الخصوصية، والمحافظة عليها.

على خط متصل، أثار اقتراح قانون حول "الأمن في الفضاء السيبيري"، في الولايات المتحدة الأميركية، عددا من الاحتجاجات، نظرا للصلاحيات الواسعة، وغير المسبوقة، التي منحها للحكومة، على الإنترنت[56].

فقد وسع المقترح، فيما يتعلق بالخصوصية، دائرة الصلاحية في الوصول إلى البيانات، إلى حد تجاوز، بعض النصوص القانونية القائمة[57]، والتي تعنى بحماية البيانات الشخصية. ويعطي المقترح لوزير التجارة، حقا بالوصول إلى جميع البيانات

---

[53] - Loppsi en France et Cyber-securite aux USA http://www.natchers.com/actualite-2009/8239/loppsi-en-france-et-cyber-securite-aux-usa

[54] - Les USA se dotent d’un commandement militaire pour le cyberspace. porte parole du pentagone : « les risques lies a la cybersecurite figurent parmi les défis économiques et de sécurité nationale les plus sérieux du XXIe siecle ».
http://www.elwatan.com/Les-USA-se-dotent-d-un

[55] - Le cyberspace anglais désormais protégé par d’anciens pirates informatiques.
http://techno.branchez-vous.com/actualite/2009/06/le_cyberspace_anglais_desormais

[56] - There's a new bill working its way through Congress that is cause for some alarm: the Cybersecurity Act of 2009 (PDF summary here), The bill as it exists now risks giving the federal government unprecedented power over the Internet

[57] - The Electronic Communications Privacy Act, the Privacy Protection Act, The financial privacy regulations.

الخاصة بالبنية التحتية الحساسة Critical، دون مراعاة لأي نص قانوني، أو نظام، أو قاعدة، أو سياسة تمنع هذا الوصول.

وبالتالي، يبدو واضحا أن المقترح، كان يتجه إلى منح السلطة، حق الوصول إلى "جميع البيانات ذات الصلة"، العائدة إلى القطاع الخاص، خارج إطار "حالة الطوارئ، دون اعتبار، لضرورة حماية الحق في الخصوصية، أو للقواعد القانونية، والأصول القضائية الواجب احترامها، في الظروف العادية.

وفي العام 2015، تم إقرار قانون اتحادي، في مجلس الشيوخ، تحت عنوان "تقاسم المعلومات المتعلقة بالأمن السيبراني"، بهدف تحسين الأمن السيبراني، من خلال تعزيز تبادل المعلومات، حول تهديدات الفضاء السيبراني. ويسمح هذا القانون، للحكومة الأميركية بالحصول من الشركات الخاصة، على معلومات حركة المرور على الإنترنت. وقد اعتبر العديد من الجهات المعنية بالدفاع عن الحريات، أن هذا القانون، هو خطوة إلى الوراء فيما يتعلق بحماية البيانات الشخصية، والحق في الخصوصية، إذ يسمح بمشاركة البيانات على نطاق واسع، بين عدد من أجهزة الدول، لاسيما منها الوكالة الأميركية للأمن القومي[58].

- **الرقابة والسيطرة**

فمع دفق المعلومات، وتصاعد استخدام الهواتف الخلوية، وغيرها الكثير من الأجهزة المتصلة بالإنترنت، وتضخم إمكانات الاتصال، تحول كل فرد، إلى لاقط عند أجهزة الاستخبارات الدولية[59].

[58] - The Cybersecurity Information Sharing Act of 2014 (CISA) (S. 2588) takes a significant step back from the privacy protections that were included in the last cybersecurity information-sharing bill considered by the Senate, the Cybersecurity Act of 2012 (S. 3414). It also fails to address the significant concerns that have been raised over the last year as Americans have learned about the scope and breadth of the government's surveillance and cyber operations.
http://akdev.preview.newamerica.org/oti/oti-analysis-of-cybersecurity-information-sharing-act-cisa-s-2588/

[59] - We are "somehow becoming a sensor for the world intelligence community" - Philippe Langlois- founder of the Paris-based company Priority One Security, on agencies' ability to harvest personal data from users of smartphones.
http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

وتستخدم العديد من الدول، برامج رقابة متطورة، تقارن بين ما تسلمه إياه، شركات الاتصال الكبرى، وما جمعته ألإدارات والأجهزة الحكومية، من بيانات ولوائح، ومن معلومات نتيجة تعقب الأفراد عبر تطبيقات تحديد المواقع، والوصول إلى لوائح أصدقائهم، وأفراد عائلتهم، وبيانات اتصالاتهم، والبيانات الجغرافية الموجودة على الصور، والتي يتبادلونها على مواقع التواصل الاجتماعي، عبر هواتفهم، وبريدهم الإلكتروني. وكانت أجهزة الاستخبارات البريطانية، قد أشارت في مستندات سرية، إلى أن القدرة على التجسس، موجودة في برامج الألعاب الأكثر انتشارا، لاسيما عندما تسمح بتحديد موقع الشخص، وعمره، وجنسه، وغير ذلك من بياناته الشخصية[60].

وتجدر الإشارة هنا، إلى ما يمثله هذا الواقع، من تهديد جدي للحياة الخاصة، ومن خلالها للحريات المدنية، والحقوق الشخصية الأخرى، التي تعتبر أساسية في إرساء قواعد الديمقراطية، والحكومة الرشيدة[61].

وفي هذا الإطار، تحتل أخبار انتهاك الحق في الخصوصية، والحريات المدنية، وحرية التعبير على الإنترنت، الصفحات الأولى، في وسائل الإعلام. وتنتشر، أخبار تعامل الأجهزة الحكومية المختلفة، مع البيانات الشخصية والمعلومات، من منطلق ضرورة الرقابة والسيطرة.

---

[60] - Lisa Vaas on January 29, 2014- Spy agencies are slurping personal data from leaky mobile apps- http://nakedsecurity.sophos.com/2014/01/29/spy-agencies-are-slurping-personal-data-from-leaky-mobile-apps/- consulted on 30/1/2014

- A secret British intelligence document, from 2012, said that spies can scrub smart phone apps to collect details, like a user's "political alignment", and sexual orientation.

[61] - "The right to privacy, the right to access to information and freedom of expression are closely linked. The public has the democratic right to take part in the public affairs and this right cannot be effectively exercised by solely relying on authorized information." Ms. Pillay- UN High Commissioner for Human Rightshttp://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

فمن ويكيليكس[62]، إلى تامبورا[63] في بريطانيا، إلى سنودين[64] وبريسم[65] في الولايات المتحدة الأميركية، إلى برامج الاستخبارات في كندا[66]، إلى تشديد الرقابة على الإنترنت في فنزويلا[67]، وسورم 2، وسورم 3، والسجل الواحد في روسيا[68]، واتخاذ إجراءات تضمن تحديد هوية الأشخاص[69]، وحجب مواقع التواصل الاجتماعي، والجدار العظيم في الصين[70]، تأكيد على لجوء الحكومات المختلفة، إلى ممارسة الرقابة الشاملة، سواء على المستوى الوطني، أم على المستوى الخارجي، وعلى استغلال البيانات الشخصية، في عمليات رقابة، ورصد تحركات، لم يسبق لها مثيل، في تاريخ الإنسانية، وممارسات الدول.

فمع ازدياد المكننة، وانتشار الأجهزة المتصلة بالإنترنت، وبروز إنترنت الأشياء، والحوسبة السحابية، تضاعفت تهديدات الحق في الحفاظ على الحياة الخاصة، وتوسعت آفاق الرقابة، إلى أن تحولت إلى رقابة شاملة، أدت فيما أدت، إلى ردات فعل لدى الرأي العام، بلغت ذروتها، مع الفضيحة التي فجرها إدوارد سنودين في العام 2013، حول الرقابة التي تقوم بها أجهزة الاستخبارات الأميركية، ليس

[62] - https://wikileaks.org/

[63] - Tempora, is a clandestine security electronic surveillance program tested in 2008,[2] established in 2011 and operated by the British Government Communications Headquarters (GCHQ). Tempora uses intercepts on the fibre-optic cables that make up the backbone of the internet to gain access to large amounts of internet users' personal data. http://en.wikipedia.org/wiki/Tempora

[64] - http://edition.cnn.com/2013/09/11/us/edward-snowden-fast-facts/
- En juin 2013, l'informaticien de la National Security Agency (NSA) américaine, Edward Snowden, révélait l'existence de programmes de surveillance. Le plus connu, nommé PRISM, permet au gouvernement américain d'accéder directement aux serveurs de neuf compagnies: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple. La NSA aurait ainsi, en mars 2013, récupéré 97 milliards d'informations. http://www.la-croix.com/Actualite/Monde/Pourquoi-il-faut-reformer-Internet-2014-04-23-1140281

[65] - Special source operation system legally immunized private companies that cooperate voluntarily with U.S. intelligence collection.

[66] - Attention fliers: Canada's electronic spy agency is following you - new Snowden leaks.http://rt.com/news/canada-snowden-spying-nsa-airport-442/

[67] - Venezuelan Government Expands Internet Censorship- http://mashable.com/2014/02/20/venezuela-social-media/

[68] - In Ex-Soviet States, Russian Spy Tech Still Watches You-By Andrei Soldatov and Irina Borogan- 12.21.12- 6:30 AM - http://www.wired.com/dangerroom/2012/12/russias-hand/all/

[69] - China orders real name register for online video uploads. http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121

[70] - King, Gary, Jennifer Pan, and Margaret Roberts. 2014. Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation. Copy at http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

فقط على الأجانب، وإنما أيضاً على المواطنين الأميركيين[71]. فلقد اصبح واضحا للعالم، أن التقدم التكنولوجي، لا يمر دون مخاطر جديدة، على الحريات والحقوق، وان ممارسات القطاعين العام والخاص، تشكل تهديداً أكيداً، وتطرح تحديات، لا يمكن للمشترع تجاهلها، دون الإساءة إلى الإنسان، وإلى القيم والأخلاقيات الإنسانية.

وكانت تصريحات سنودين، بما كشفته من عمليات تجسس في الولايات المتحدة الأميركية، على الديبلوماسيين، والسياسيين، والمواطنين، كما الأجانب، قد أثارت موجة من الاستياء، حول العالم، أدت فيما أدت، إلى قيام الرئيسة البرازيلية، بالدعوة لعقد قمة دولية حول مستقبل الإنترنت، تناقش فيها، بشكل أساسي، حقوق الدول المختلفة في سياسة إدارة الإنترنت، وحماية الحقوق، لاسيما الحق في الخصوصية، وحماية البيانات الشخصية[72].

وعليه، إن تحول الرقابة، إلى رقابة شاملة Mass Surveillance، والتحكم بوسائل الاتصالات المختلفة، وجمع البيانات عنها، لتعقب الأفراد والمؤسسات، تهدد الحريات، بدءا من حرية المعتقد، مرورا بحرية الرأي والتعبير،التي تقرها الدساتير في الدول عامة، وصولا إلى حرية ممارسة النشاط السياسي والاجتماعي، بما يهدد الاقتصاد ونموه[73]، إضافة إلى تقويضه أسس النظام الديمقراطي[74]. وفي كل

[71] - NSA files decoded.
https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

[72] - Pourquoi il faut réformer Internet
http://www.la-croix.com/Actualite/Monde/Pourquoi-il-faut-reformer-Internet-2014-04-23-1140281

[73] - The NSA overreach poses a serious threat to our economy-
http://www.theguardian.com/commentisfree/2013/nov/20/jim-sensenbrenner-nsa-overreach-hurts-business
UNGA- 16 May 2011 A/HRC/17/27- Human Rights Council- Seventeenth session- Agenda item 3 - Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development "The growing use and sophistication of digital surveillance has outstripped the ability of societies to legislate their proper use, leading to "ad hoc practices that are beyond the supervision of any independent authority," and that threaten to repress free expression"

[74] - UNGA- 16 May 2011 A/HRC/17/27- Human Rights Council- Seventeenth session- Agenda item 3 - Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development "The growing use and sophistication of digital surveillance has outstripped the ability of societies to legislate their proper use, leading to "ad hoc practices that are beyond the supervision of any independent authority," and that threaten to repress free expression"

ما تقدم، دليل على أهمية البيانات الشخصية، وضرورة حمايتها، لمنع استغلالها في الإساءة إلى حقوق الأفراد، وفي الوصول إلى مستخدمي وسائل الاتصالات، دون وجه حق.

وقد اعتبر القضاء الأميركي، أن هذه الرقابة الشاملة، تشكل تعديا صريحا على الحريات. ففي قضية مرفوعة من الاتحاد الأميركي للحريات المدنية، ضد عدد من الأجهزة الأمنية والاستخباراتية، ووزير الدفاع، على خلفية التنصت على المواطنين الأميركيين، وجمع بيانات اتصالاتهم وبياناتهم الشخصية، اعتبرت محكمة في نيويورك، أن هذا العمل، يخرج عن الصلاحيات المعطاة لهذه الهيئات، في إطار مهمتها لحفظ الأمن القومي، ويخالف التعديلين الأول والثاني من الدستور، اللذين يقران حرية التعبير، وحق الشخص في عدم انتهاك حرمة مسكنه، دون وجه حق[75].

حركة التشريع: أطر الحماية

تأثرت حركة حماية البيانات الشخصية، على المستوى القانوني، منذ بروزها، بتطور تقنيات المعلومات والاتصالات، مع بدء مكننة الإدارات الرسمية، والمؤسسات الخاصة، وبروز إمكانات تحديد هوية الشخص، من خلال رقم تعريفي، أو هوية رقمية موحدة. وقد أدى ذلك، إلى إثارة هواجس لدى المواطنين، الأمر الذي استدعى تحرك المشترع، لاسيما في أوروبا، لإقرار حماية الحياة الخاصة، والحريات الفردية، في مواجهة المكننة.

ففي فرنسا مثلا، شهدت بداية السبعينيات وعياً لإمكانيات الحوسبة الهائلة، وولادة مشروع وطني، عرف بالنظام الآلي للملفات الإدارية ودليل الأفراد، SAFARI[76]، بهدف تحديد هوية كل مواطن من خلال معرف، يؤمن تقاطع

[75] - United states district court southern district of New York. 13 Civ. 3994- June 11 2013- https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf

[76] - SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus)

الملفات الموجودة في كافة الإدارات الفرنسية، وذلك دون المرور بالبرلمان. وقد أثار هذا الأمر، اعتراض العديد من الأفراد، والمسؤولين، الذين رأوا فيه، وسيلة للاعتداء على حقوق الفرنسيين[77]. وتعتبر المخاوف التي أثارها هذا المشروع، الدافع الأساسي، لإقرار أولى قوانين حماية الأشخاص الطبيعيين، من المعالجة الآلية للبيانات الشخصية، وإنشاء الهيئة الوطنية للمعلوماتية والحريات.

ثم، ومع انطلاق الشبكة العالمية للمعلومات، وتدفق البيانات، تحولت هذه الأخيرة، إلى محرك للاقتصاد، وقيمة تسعى إليها مختلف الشركات، وعامل أساسي، في تقديم الخدمات الصحية، وفي تطوير أساليب العمل والإدارة، وفي حركة جمع المعلومات، من قبل أجهزة الاستخبارات.

- **في الغرب**

مع وعي إمكانات التكنولوجيا، وأهمية دور الإنترنت، وطبيعتها، انصب الاهتمام التشريعي، على حماية البيانات الشخصية، لمنع التعرض لحقوق الأفراد، ولكن مع المحافظة على حرية دفق المعلومات. لذا تنبهت الدول إلى ضرورة التعاون، والسعي إلى تحقيق نوع من الانسجام، يضمن تحقيق هذه الأهداف، ويؤمن بيئة آمنة، لحركة البيانات التي باتت تعبر الحدود الوطنية، لتنتشر في العالم. وقد برزت في هذا السياق، جهود عدد من المنظمات الدولية، إضافة إلى الجهود الأوروبية، التي تجسدت، في عدد من التوصيات، والإرشادات، والاتفاقيات بين دول الاتحاد الأوروبي، لحماية الأشخاص الطبيعيين، في مواجهة قدرة التقنيات الحديثة، على تهديد حقوقهم وحرياتهم، ولدعم حركة تبادل المعلومات.

[77] - Et de l'informatisation de ces fichiers, voilà ce qu'il écrit: «De telles visées comportent un danger qui saute aux yeux et que M. Adolphe Touffait, procureur général de la Cour de Cassation avait parfaitement défini le 9 avril 1973 devant l'Académie des sciences morales et politiques en disant: «la dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés et même à l'équilibre des pouvoirs politiques»
http://www.getavocat.fr/blog/2018/02/17/protection-des-donnees-personnelles-ces-lanceurs-d-alerte-meconnus-de-1974.html

- على المستوى الفردي

وهكذا، ارتبط الحق في حماية البيانات الشخصية، منذ نشأته، بالحق في الحفاظ على الحياة الخاصة.

ففي العام [78]1974، صدر قانون الخصوصية في الولايات المتحدة الأميركية، حول الممارسات العادلة لجمع، وحماية، ونشر، واستخدام البيانات الشخصية، التي تحفظ في سجلات دوائر الحكومة الفدرالية، حيث يمكن استخراج معلومات باستخدام اسم الشخص، أو أداة تعريف عنه، كرقم هويته، أو سجله الطبي. وقد منع هذا القانون، كشف بيانات شخص معين، دون الحصول على موافقته الخطية، ما عدا الحالات ألاثنتي عشرة المحددة قانونا[79]، والتي ترتبط ارتباطا وثيقا، بحاجة الإدارة إلى إرساء الاستقرار الاجتماعي، والاقتصادي، والصحي، والأمني في البلاد. وكانت جميع قوانين الحماية، التي صدرت حول العالم، تستعيد بعضا منها، لتبرر كشف هذه البيانات، تحت عناوين المصلحة العامة، والأمن، والمصلحة الشخصية لصاحب البيانات، وغير ذلك، مما سنعرض له لاحقا.

وقد اقر هذا القانون، عددا من الحقوق لصاحب البيانات، تسمح له بممارسة حقه في إدارة بياناته، من خلال حقه في الاطلاع على السجلات، وطلب تعديل وتصحيح البيانات، ومعرفة ما الذي جمع أو نشر عنه من معلومات.

أما هدفه، كما نصت على ذلك المادة الأولى منه، فهو إعادة التوازن بين حق الدولة في جمع البيانات الشخصية، وحق الفرد في حماية حياته الخاصة، من التدخل غير المشروع للدولة، والذي يمكن أن ينتج عن كشف هذه البيانات

---

[78] - The Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a)

[79] - Conditions of Disclosure to Third Parties
A. The "No Disclosure Without Consent" Rule
B. Twelve Exceptions to the "No Disclosure Without Consent" Rule
5 U.S.C. § 552a(b)(1) ("need to know" within agency), 5 U.S.C. § 552a(b)(2) (required FOIA disclosure), 5 U.S.C. § 552a(b)(3) (routine uses), 5 U.S.C. § 552a(b)(4) (Bureau of the Census), 5 U.S.C. § 552a(b)(5) (statistical research), 5 U.S.C. § 552a(b)(6) (National Archives), 5 U.S.C. § 552a(b)(7) (law enforcement request), 5 U.S.C. § 552a(b)(8) (health or safety of an individual), 5 U.S.C. § 552a(b)(9) (Congress), 5 U.S.C. § 552a(b)(10) (General Accounting Office), 5 U.S.C. § 552a(b)(11) (court order), 5 U.S.C. § 552a(b)(12) (Debt Collection Act)

وإساءة استخدامها، في وقت ازداد فيه استخدام الإدارة لتقنيات معالجة البيانات الشخصية، وحفظها، واستخراجها عبر معرف شخصي موحد، كرقم بطاقة الضمان الاجتماعي. بينما، تعود حماية البيانات الشخصية، خارج إطار ممارسات الحكومة الفدرالية، إلى كل ولاية، وتخضع لصلاحية محاكمها، على ما أقرته المحكمة العليا، في قرار صادر في العام 1965[80].

وفي العام 1978، صدر تشريع فرنسي، بعنوان: "المعلوماتية، الملفات، والحريات"، فحددت المادة الأولى الهدف من المعلوماتية، على انه خدمة لكل مواطن، واعتبرت أن إطار تطويرها، يجب أن يتم عبر قنوات التعاون الدولي، مع الالتزام بالامتناع عن استخدامها للتعرض للهوية الإنسانية، أو لحقوق الإنسان، أو الحياة الخاصة، أو الحريات الفردية والعامة. كما أقرت هذه المادة، حق كل شخص، في اتخاذ القرار، وفي السيطرة على استخدامات بياناته الشخصية، بحسب أحكام القانون.

« تقرير مجلس شورى الدولة الفرنسي

ولأن بدايات التشريع، كانت اكثر بروزا، في أوروبا، ولان فرنسا، هي البلد الأول الذي انشأ هيئة وطنية لحماية البيانات الشخصية، فلا بد من التوقف، عند مقترحات مجلس الشورى الفرنسي، في تقريره السنوي، الصادر في التاسع من أيلول/سبتمبر [81]2014، تحت عنوان "الرقمية والحقوق".

أما الأسباب الداعية لذلك، فمنها، انه الجهة الموكل إليها، حماية الحريات، والحقوق الأساسية، ولان التقرير قد بحث بعمق، في التحولات التي يشهدها المجتمع، نتيجة التطورات الرقمية، والتقدم التقني، وأثر ذلك على حقوق الأفراد، والمواطنين، ولأنه خلص إلى عدد من الاقتراحات الضرورية، التي وجهها إلى الحكومة،

---

[80] - https://supreme.justia.com/case/federal/us/381/479/case.html

[81] - Accueil / Décisions, Avis & Publications / Études & Publications / Rapports & Études / Étude annuelle 2014 - Le numérique et les droits f. 9 septembre 2014 - Étude annuelle 2014 - Le numérique et les droits fondamentaux 50 propositions du Conseil d'État pour mettre le numérique au service des droits individuels et de l'intérêt général.

لتسخير التقنية، في خدمة المواطن، وتحقيق توازن، يمكنه أن يضمن ذلك.

ويكون التقرير، قد شمل بذلك، معظم أوجه المسائل، التي تتطرق إليها قوانين الحماية، كالمبادئ، والحقوق، والموجبات القانونية والتقنية، وصلاحيات هيئات الحماية، إضافة إلى البعد الدولي لنقل البيانات، والعلاقة القانونية، بين الدول.

فقد أشار التقرير، إلى التحول الذي طرأ، على شروط ممارسة الحقوق والحريات الأساسية الجديدة، وعلى أسلوب ممارستها، والتمتع بها، نتيجة إنفلاش الاعتماد، على تقنيات المعلومات والاتصالات. وقد دعا في هذا السياق، إلى إعادة النظر في الإطار التنظيمي والقانوني، الذي يحميها، بهدف وضعها في خدمة الحقوق الفردية، والمصلحة العامة.

قسمت هذه المقترحات، حسب محاورها، إلى ما يتصل بالحقوق الأساسية، وتعزيز حقوق الأفراد والمجموعات، وإعادة تحديد أطر الحماية القانونية، والتنظيمية، والتفكير في الدور الفاعل للسلطات العامة، وضمان الحقوق الأساسية في مواجهة تحول الإدارة العامة إلى الرقمية، وتنظيم العلاقات، بين الاتحاد الأوروبي، والدول الأخرى.

لكن الأهم، هو انه أكد على ضرورة إعادة النظر، ليس فقط في دور السلطات العامة، وإنما أيضا، في المبادئ التي تقوم عليها حماية الحقوق الأساسية، بما يساعد على تعزيز مكانة الفرد، في الدفاع عن حقوقه.

وقد ارتأى المجلس، لهذه الغاية، إعادة التفكير، في تعزيز قدرة الفرد في مواجهة الاستخدامات المختلفة لبياناته، وفي دور السلطات العامة، وفي كيفية إيجاد التوازن على مستوى القانون الدولي، بين مبدأي "وطن الشخص المعني"، و"وطن الموقع الإلكتروني"، أي في جعل قانون متلقي الخدمة، هو المطبق، بغض النظر، عن بلد الموقع.

ويبدو، إن القواعد الأوروبية الجديدة، التي وضعت في العام 2016، قد اعتمدت هذا المقترح، حيث أقرت تطبيق القانون الأوروبي، خارج الاتحاد، لحماية بيانات الأوروبيين[82].

وقد دعا، بالإضافة إلى ذلك، إلى تعزيز الأمن القانوني، لاستخدام البيانات، والإشراف عن كثب، على عمليات معالجتها، والتي يمكن أن تشكل تهديدات أكثر خطورة، من غيرها، مشددا على ضرورة منح الهيئة الوطنية للمعلوماتية والحريات، وجميع السلطات الأوروبية لحماية البيانات، تفويضاً واضحًا، لتعزيز التقنيات التي تؤمن سيطرة الأفراد، على استخدام البيانات الشخصية.

وإذا كان المجلس، قد استبعد فكرة إعطاء الشخص المعني، حق الملكية على بياناته، إلا انه قد اقترح اللجوء إلى مبدأ "تقرير المصير المعلوماتي"؛ بمعنى أن يمنح الفرد، حرية وحق تقرير، تسليم بياناته الشخصية، والسماح باستخدامها.

كذلك، رأى المجلس ضرورة الترويج لاقتصاد بيانات شخصية مسؤول، عبر تطوير الضمانات التقنية والإدارية المناسبة، لإخفاء الهوية، التي تمنع إعادة تحديد الهوية، والتي يمكن أن تسمح بإعادة الاستخدام الإحصائي لهذه البيانات، بغض النظر عن الغرض الأصلي.

وعلى المستوى القانوني، الذي يختص بتنظيم الأطراف المعنية بإدارة الخدمات، وتقديمها على الإنترنت، طرح إنشاء فئة قانونية جديدة لـ"المنصات"، متميزة عن كل من الناشرين، ومقدمي خدمات الاستضافة، تنحصر مهامها، في تقديم خدمات

[82] - Article 3 - Territorial scope
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

الترتيب، أو الرجوع للمحتوى، أو السلع، أو الخدمات، التي تنشرها أطراف أخرى. وتخضع هذه الفئة، في علاقتها مع المستخدمين، لمبدأ الشرف، أو الولاء.

ويقضي هذا المبدأ، بان الأطراف، التي وافقت على اعتبار العقد بينها، ملزما أثناء فترة انعقاده، لا يمكنها أثناء المحاكمة، أن تدعي وجود مخالفة تبطل هذا العقد، أو تلغي مفاعيله، بهدف التهرب من الالتزامات، التي ينص عليها.

- **على المستوى الجماعي**

وأبرز ما سجل في هذا المجال: توصيات منظمة التعاون الاقتصادي، قرار الجمعية العامة للأمم المتحدة، رقم 45/95، والقواعد الأوروبية الجديدة.

» **توصيات منظمة التعاون**

لعبت منظمة التعاون الاقتصادي والتنمية، منذ منتصف السبعينيات من القرن الماضي، دوراً أساسيا، في تعزيز احترام الحق في الخصوصية، كقيمة أساسية، وشرط لضمان التدفق الحر للبيانات الشخصية، عبر الحدود، فأقرت قواعد إرشادية لحماية هذا الحق، والحركة الحرة لتدفق البيانات.

وقد أصدر مجلس المنظمة، في العام 1980، توصيات إلى البلدان الأعضاء، تحت عنوان حماية الحياة الخاصة، وتدفق البيانات الشخصية عبر الحدود، قدم لها، بضرورة احترام الحياة الخاصة والحريات الفردية؛ باعتبار هذا الأمر من مصلحة الدول الأعضاء، والتوفيق بين القيم الأساسية، التي يمكن أن تتعارض؛ كالحق في الخصوصية، والانسياب الحر للمعلومات.

كما أظهرت المقدمة، اعتبار المجلس، أن التدفق الحر للبيانات الشخصية عبر الحدود، من العوامل المساهمة في النمو الاقتصادي والاجتماعي، بما يفرض على الدول الأعضاء، الاهتمام بضمان حماية البيانات الشخصية، والحياة الخاصة، والحريات

الفردية، في إطار قوانين وتنظيمان منسجمة، تمنع إعاقة حركة تدفق البيانات عبر الحدود.

وعلى أثر هذه التوصية، صدرت في أوروبا، اتفاقية عام 1981، وحملت الرقم 108، بهدف التوفيق بين حرية تبادل المعلومات، والمبادئ الأساسية لحماية الحياة الخاصة. اعتبرت هذه الاتفاقية، أول نص ملزم دوليا، يتعين بموجبه على الدول الأعضاء، اتخاذ الخطوات اللازمة، على المستوى التشريعي، لتطبيق المبادئ التي تحددها، والتي تهدف إلى ضمان احترام حقوق الإنسان الأساسية، للجميع من دون استثناء.

وقد وقعت هذه الاتفاقية، من قبل دول غير أعضاء في الاتحاد الأوروبي، منها دول عربية، كتونس والمغرب. كما وقعتها الأرجنتين، والمكسيك، والأوروغواي، وبوركينا فاسو، غيرها.

» **قرار الجمعية العامة رقم 45/95**

صوتت الجمعية العامة للأمم المتحدة، بتاريخ 14 كانون الأول 1990، على قرار حمل الرقم 45/95، تضمن المبادئ التوجيهية، لتنظيم ملفات البيانات الشخصية، المعدة بالحاسبة الإلكترونية. وقد لحظت هذه المبادئ، مجمل مسائل الحماية، عبر نطاق تطبيقها، والذي يشمل جميع الجهات المعنية، بجمع البيانات ومعالجتها، سواء أكانت بيانات عامة أم خاصة، وعبر الدعوة، إلى توسيع نطاق التطبيق، ليشمل الأشخاص المعنويين، إضافة إلى الأشخاص الطبيعيين.

كما تطرقت إلى هذه المسائل، على المستوى الوطني، من خلال المبادئ، التي يجب إقرارها، والاستثناءات، وضرورة تعيين سلطات الرقابة، والعقوبات الجزائية، وعلى المستوى الدولي، من خلال أصول ومبادئ تدفق البيانات عبر الحدود، وقابلية تطبيق المبادئ على المنظمات الدولية الحكومية، وغير الحكومية.

أما المبادئ، التي تلتزم الدول المعنية بإيرادها في قوانينها، فهي:

- مبدا المشروعية والنزاهة، الذي يمنع جمع وتجهيز البيانات الشخصية، بأساليب غير نزيهة أو غير مشروعة، ويدعو إلى الالتزام باستخدامها، بما ينسجم مع مقاصد ميثاق الأمم المتحدة، ومبادئه.
- مبدأ صحة البيانات، الذي اعلن مسؤولية معالجي ملفات البيانات، والمحتفظين بها، عن التحقق من دقة البيانات، وتيويمها، والتأكد من ملاءمتها، للغاية التي عولجت لأجلها.
- مبدأ تحديد الغاية، الذي أقر: مبدأ الإعلان المسبق عن هدف جمع البيانات ومعالجتها، على أن يكون هذا الهدف مشروعا ومحددا، بما يسمح بممارسة رقابة لاحقة، تضمن التأكد من: عدم الانحراف عن الغاية المعلنة، احترام حق الشخص المعني في الموافقة على استخدام البيانات، وإفشاء الشخصية العائدة له، والالتزام بمحو البيانات بعد إنجاز الهدف المحدد.
- مبدأ وصول الأشخاص المعنيين إلى الملفات، والذي اقر حق المعني في الاطلاع على كيفية التصرف ببياناته، وطرق استخدامها، إضافة إلى حقه في إعلام واضح، دون تكبيده أي كلفة غير مبررة، وحقه في طلب تصحيح البيانات، أو محوها.
- مبدأ عدم التمييز، الذي ينطلق من مبدأ عدم جواز التمييز العنصري، بناء على بيانات شخصية، حول العرق، أو الأثنية، أو اللون، أو الميول الجنسية، أو الآراء السياسية، أو المعتقدات الدينية والفلسفية، أو العضوية النقابية والمهنية.
- مبدأ الأمن، الذي يلزم المعنيين بعمليات جمع البيانات وحفظها، اتخاذ التدابير الملائمة لمنع فقدان البيانات، أو تلفها، أو تسربها، أو الاطلاع عليها، نتيجة لعوامل طبيعية، أو لتصرفات بشرية غير مشروعة، كالدخول إلى الأنظمة دون إذن، أو استخدامها بشكل غير آمن.

وقد دعت هذه المبادئ، إلى إنشاء سلطة رقابة، تتولى الإشراف على احترام المبادئ السالفة الذكر، وكيفية تطبيقها، كما دعت إلى إقرار عقوبات جزائية، وآليات تضمن إمكانية ملاحقة المخالفين.

كذلك، أشارت إلى ضرورة أن تعمل الدول، على أن تشمل هذه المبادئ، المنظمات الدولية الحكومية، وغير الحكومية، عبر وضع القوانين اللازمة، التي تلزمها احترام مبادئ حماية البيانات الشخصية، وحقوق الأشخاص المعنيين بها، وتأمين آليات تضمن حقهم في ملاحقة الأعمال التي تتعارض وحقهم، في المحافظة على بياناتهم صحيحة ودقيقة، وفي عدم استخدامها بطريقة غير مشروعة، وعدم تسريبها.

» القواعد الأوروبية الجديدة لحماية البيانات

من هنا، كان من البديهي، أن يعود النقاش، حول ضرورة حماية الحق في الخصوصية، مع إقرار الحق في طلب محو البيانات الشخصية، كضمانة للحق في النسيان، وعلاقته بالبيانات التي تجمع سرا، وتنشر دون تحفظ على الإنترنت، والتي يتم بيعها وتداولها، دون معرفة صاحبها.

فالبيئة التشريعية المربكة والمعقدة، في الاتحاد الأوروبي، والتي كانت تتألف من 28 تشريعا وطنيا لحماية البيانات الشخصية، لم تعد ملائمة لحركة التطور السريعة، ولتصاعد أنواع التهديدات، التي يتعرض لها، سواء الأفراد، أو المنظمات، أو الشركات العاملة في أوروبا أو في خارجها، لصعوبة مواجهتها، وللكلفة التي تفرضها، لناحية الوقت والمال، والحاجة إلى مواكبة الالتزامات والموجبات، التي تفرضها. إذ تعود هذه القوانين، إلى القواعد الإرشادية الصادرة في العام 1995؛ أي في وقت كان عدد مستخدمي الإنترنت من الأوروبيين، لا يتجاوز الـ3%، وكان تدفق المعلومات والبيانات، لم يبلغ الحجم الهائل، الذي بات اليوم، يحسب بالزيتا بايت ZettaBytes.

في هذا السياق، صدرت القواعد الأوروبية عن البرلمان والمجلس الأوروبيين، في

27 أبريل 2016، لتنظم حماية الأشخاص الطبيعيين، من المعالجة الرقمية للبيانات الشخصية، والتدفق الحر للمعلومات.

وقد دخل التشريع الأوروبي الموحد، حول حماية البيانات الشخصية، حيز التنفيذ، في أيار / مايو 2018، تحت عنوان: "القواعد العامة لحماية البيانات". وهو يهدف، إلى تحقيق الانسجام بين القوانين الأوروبية، الخاصة بحماية البيانات، عبر توحيد التشريع، بما يخدم تعزيز الشفافية، لدعم حقوق الأفراد، ونمو الاقتصاد الرقمي.

فمما لا شك فيه، أنه من المهم للشركات التجارية، التي تعمل ضمن السوق الأوروبية الواحدة، أن تتجنب صعوبات مواكبة القوانين الأوروبية الوطنية المختلفة. فإضافة إلى توفير مساحة اكبر للحماية، بما يساهم في رفع معدل الثقة، تجد الشركات سهولة اكبر، في الالتزام مع تشريع أوروبي واحد، يطبق في مختلف دول الاتحاد.

كما يستجيب هذا التشريع، لحاجة مركزية: بناء الثقة والأمان في الفضاء السيبراني، من جهة أولى، و مواكبة التطورات المتسارعة، في مجال تقنيات المعلومات، من جهة أخرى، حيث لم يعد ممكنا، توقع المدى الذي تبلغه قدرات تكنولوجيا معالجة المعلومات، ولا نتائج الجمع بين تقنيات مختلفة ومتنوعة، سواء على حرمة الحياة الشخصية، أوعلى أمن الدول، التي تجمع وتعالج وتتبادل، البيانات الشخصية.

أدخلت القواعد الأوروبية الجديدة، تغييرات عميقة وجذرية، إلى البيئة القانونية لحماية البيانات الشخصية، والحق في حماية الحياة الخاصة، عبر إرسائها نظاما صارما، يرتكز إلى حقوق الإنسان الأساسية، وإلى تحديات العالم الرقمي.

فقد فرض التشريع الجديد، قواعد جديدة لحماية البيانات، واحترام حقوق أصحابها، على الشركات، والإدارات الحكومية، والمنظمات بجميع أشكالها القانونية، والتي تقدم خدمات لمواطنين أوروبيين، أو لمقيمين في الاتحاد الأوروبي، أو التي تجمع بياناتهم وتعالجها، حتى ولو كان مقر إقامتها خارج الاتحاد الأوروبي.

كما يتيح هذا التشريع، فرصة أمام صاحب البيانات الشخصية، لاستعادة السيطرة عليها، ويفتح أمامه مجالا أوسع، لمتابعة ما ينشر منها، وما يتم تبادله، أو الوصول إليه، لاسيما مع إقرار عدد من الحقوق الجديدة، كالحق في النسيان، والحق في معرفة أهداف المعالجة، حتى من قبل المراقب أو المسؤول عن المعالجة، الذي لم يتول شخصيا جمع البيانات.

فمن جديد هذا التشريع، على سبيل المثال، حق المواطن أو المقيم في بلدان الاتحاد، في طلب نسخة إلكترونية عن بياناته، يمكنه الاطلاع عليها وقراءتها. فتحميل البيانات دون التمكن من الاطلاع عليها، لا يفيد. علما إن هذا يعني، منحه إمكانية التعرف إلى نماذج حركته على الإنترنت؛ كعدد الرسائل البريدية التي يرسلها، أو عدد المرات التي يزور فيها مواقع التواصل الاجتماعي، والمدة التي يقضيها على محركات البحث، والمواضيع التي يبحث عنها، والموسيقى التي يحملها، الخ...

والحصول على البيانات،بهذه الطريقة، يعني أيضاً، إمكانية إعادة استخدامها، من خلال تحميلها على موقع، أو تطبيق آخر، غير الذي كان يستخدمه صاحب البيانات.

وتختلف القواعد الجديدة عن القواعد الإرشادية التي كانت معتمدة، منذ العام 1995، بكونها تتمتع بقوة القانون، دون الحاجة إلى إصدار قوانين وطنية لإعطائها القوة التنفيذية، أو لوضع تشريع وطني يتناسب معها[83]، وذلك، حسب منطوق المادة 99، التي نصت على سريان مفعوله، بكل مندرجاته وأحكامه، في جميع الدول الأعضاء، بعد انقضاء 20 يوما، على نشره في الجريدة الرسمية للاتحاد

[83] - Art. 99 - 1. Le présent règlement entre en vigueur le vingtième jour suivantcelui de sa publication au Journal officiel de l'Unioneuropéenne., 2. Il est applicable à partir du 25 mai 2018. Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État Membre.

الأوروبي. ومن شأن هذه القواعد، والتي حددت المادة الأولى[84]، الهدف منها وغرضها، إرساء أحكام خاصة بحماية البيانات الشخصية، للأفراد الطبيعيين، في مواجهة المعالجة الرقمية، من جهة أولى، وأحكام خاصة بالتدفق الحر للبيانات، من جهة ثانية، ضمن إطار احترام الأفراد، وحقوقهم الأساسية، التي تقرها شرع حقوق الإنسان، الدولية والإقليمية.

على مستوى آخر، يهدف هذا التشريع، إلى تنسيق التشريع حول حماية البيانات، على جميع أراضي الدول الأعضاء في الاتحاد الأوروبي، إلا أن هذا لا يعني، حصر مفعوله، على هذه الأراضي، لان تبعات الالتزام به، سيكون لها تأثيرات مباشرة، أو غير مباشرة، على شركات تعمل خارج الاتحاد.

وسيكون على الشركات، إضافة إلى اعتمادها سياسات حماية مناسبة، أن تلحظ آليات جديدة، للتنقيب عن البيانات، ولاكتشافها، والإبلاغ عن الانتهاكات، والتفاعل مع الجمهور، وتحسين شروط امن أنظمة البيانات لديها. كما سيتعين على الشركات غير المقيمة، تعيين ممثل لها، في الاتحاد الأوروبي، لضمان تنفيذ مندرجات التشريع.

فلو استخدم مواطن، أو مقيم في الاتحاد الأوروبي، خدمة أو تطبيقا للاتصالات على هاتفه الخلوي، من خارج الاتحاد الأوروبي، فان معالج البيانات التي تجمع من هذا التطبيق، سيكون مسؤولا عن ضمان حمايتها، وعرضة للمساءلة، في حال تعرضها للانكشاف، وللعقوبة المقررة، كنسبة من أرباح شركته. وهكذا، سيكون وضع شركات السياحة والسفر، والطيران، والتأمين.

[84] - GDPR - Art. 1
1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.
2. Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier louer droit à la protection des données à caractère personnel.
3. La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

علما، أن الوضع سيزداد تأزما وصعوبة، مع وعي مستخدمي الإنترنت لحقوقهم، في المطالبة بتعويض، عما قد يلحق بهم من ضرر، نتيجة معالجة ببياناتهم، بصورة غير شرعية، أو نتيجة تسربها وانكشافها.

هذا، وتسمح الإجراءات الأمنية في حماية البيانات، بحماية اكثر فاعلية، تعزز الأمن السيبراني، للشركات والأفراد، على السواء، كما يمكن اعتبارها ميزة للعلامة التجارية للشركة، ولسمعتها.

على مستوى آخر، تعزز القواعد الجديدة، الحقوق التي أقرت في القواعد الإرشادية للعام 95، وتقر عددا من الحقوق الجديدة للأفراد. فالحصول على الموافقة، مشروط بكتابة شروط المعالجة، وأهدافها، بوضوح، وسهولة، وبعمل إيجابي، بمعنى أن الامتناع عن الجواب، أو السكوت، لا يعتبرا موافقة صريحة. كذلك، يحق لمن أعطى الموافقة على معالجة بياناته، أن يرجع عن ذلك، في أي وقت.

» نصوص عربية

في لبنان، لا يوجد نص يحكم مباشرة حماية البيانات الشخصية، ذلك أن مشروعي القانون اللذين قدما، ما زالا حتى اليوم، وبالرغم من الوعي لأهميتهما، في إدراج المجلس النيابي.

لكن المشترع اللبناني، لم يتوان عن أقرار قانون خاص، بحماية الحق في الخصوصية في مجال الاتصال، بعد أن تعالت الأصوات، مطالبة بذلك[85]، وبحماية الحريات، وبعد سلسلة من الاحتجاجات والاعتراضات، من أكثر من جهة وطرف.

عرف هذا القانون، بقانون "صون الحق بسرية المخابرات التي تجري بواسطة أية وسيلة من وسائل الاتصال"[86]. وقد تطرق في المادة الأولى منه، إلى حماية التخابر،

[85] - 2017 عام "قمع الحريات".. وختامه مارسيل غانم!
https://www.lebanondebate.com/news/362805

[86] - قانون 140 تاريخ 27 تشرين الأول 1999 معدل بالقانون 158 تاريخ 27 كانون الأول 1999

بأية وسيلة من وسائل الاتصال، معددا البريد الإلكتروني من ضمن هذه الأخيرة، ومؤكدا على الاهتمام بحماية الحياة الخاصة، والحريات. وكانت المادة التاسعة منه، أعطت الدولة، في حالات محصورة جدا، حق المراقبة والتتبع، عندما يتعلق الأمر بجمع معلومات ترمي إلى مكافحة الإرهاب، والجرائم الواقعة على امن الدولة، والجرائم المنظمة[87].

كذلك، اقر قانون الدفاع الوطني اللبناني[88]، استثنائيا، حق السلطة في التنصت على المكالمات، والاتصالات، بصورة حصرية (في حالات تعرض الوطن أو جزء من أراضيه أو قطاع من قطاعاته أم مجموعة من السكان للخطر). إلا أن هذا الأمر، يفترض أن يتم، بموجب مراسيم تتخذ في مجلس الوزراء، وبناء على طلب من المجلس الأعلى للدفاع.

علاوة على ذلك، حددت المادة 850 من هذا القانون، عقوبة من شهرين إلى سنتين، لكل شخص ملحق بمصلحة البريد والبرق والهاتف، يطلع بصفته هذه، على مراسلات أو مخابرات غير موجهة إليه. وتنزل العقوبة نفسها، به أيضاً، فيما لو أفشى مضمونها.

وفي السياق عينه، تنص مواد من قانون العقوبات اللبناني، على أحكام خاصة ب"الجرائم الواقعة على الحرية والشرف"، وتلحظ عقوبات تطاول الأعمال التي تقع ضمن دائرة "إفشاء الأسرار"، كإتلاف أو كشف رسالة أو برقية، أو كالاطلاع بالخدعة على مخابرة هاتفية[89].

---

[87] - المادة 9 من قانون 140 تاريخ 27 تشرين الأول 1999 معدل بالقانون 158 تاريخ 27 كانون الأول 1999: "لكل من وزير الدفاع الوطني ووزير الداخلية أن يجيز اعتراض المخابرات بموجب قرار خطي معلل وبعد موافقة رئيس مجلس الوزراء، وذلك في سبيل جمع معلومات ترمي إلى مكافحة الإرهاب، والجرائم الواقعة على امن الدولة، والجرائم المنظمة. يحدد القرار وسيلة الاتصال موضوع الإجراء، والمعلومات التي يقتضي ضبطها، والمدة التي تتم خلالها عملية الاعتراض، على أن لا تتجاوز هذه المدة الشهرين وعلى أن لا تكون قابلة للتمديد إلا وفق الأصول والشروط عينها.

[88] - مرسوم اشتراعي 83/102 تاريخ 1983/9/16

[89] - قانون العقوبات اللبناني -الفصل الثاني:"في الجرائم الواقعة على الحرية والشرف"النبذة الرابعة: "في إفشاء الأسرار" المواد من 579 لغاية 581.

وكان القانون 158، تاريخ 27/12/1999، قد عدل القانون 140، بعد الاعتراض الذي سجل على ضم أعضاء من البرلمان إلى الهيئة، نظرا لما يمكن أن يشكله هذا الأمر، من تعارض مع مبدا فصل السلطات، ومبدأ استقلال الهيئة. وقد منحت هذه الهيئة، صلاحيات تحقيق واسعة، تتيح لها عمليا، إنجاز مهمتها بالشكل الذي يتناسب ودورها، في صون السرية، والحفاظ على الحريات، حيث يمكنها مساءلة جميع الإدارات الرسمية والخاصة، العاملة في المجالات المتصلة بتأمين الاتصالات، وإجراء الكشف الذي ترتئيه، والاستعانة بمن تراه، والاطلاع على المعدات والمستندات اللازمة، بغض النظر عن درجة سريتها.

وقد لجأ معظم المشرعين العرب، الذين وضعوا قوانين في هذا المجال، كما أولئك الذين أعدوا مشاريع قوانين أيضا، إلى النصوص الأوروبية، وغيرها مما هو مطبق. ونذكر هنا، ما نشر حول اقتراح القانون اللبناني، لتنظيم المعاملات الإلكترونية، في لبنان، والذي التزم مبادئ التوصية الأوروبية حول حماية البيانات الشخصية، وأخذ عن قوانين غربية، واهمها التشريع الفرنسي في هذا المجال، والصادر عام 2004.

فقد ورد في هذا الاقتراح، المؤلف من 175 مادة، في المادة 30 منه، من الباب الخامس، عنوان " حماية المعلومات ذات الطابع الشخصي"، لحماية هذه المعلومات. وقد توزع على خمسة فصول، عناوينها: الأحكام العامة، وعمليات جمع ومعالجة المعلومات، والإجراءات الخاصة بتنفيذ هذه الأخيرة، وحق الوصول والتصحيح، والأحكام الجزائية التي تطاول مخالفة الأحكام الخاصة بحماية المعلومات.

وكانت دبي التي أقرت "قانون حماية البيانات الشخصية في العام 2007، وعينت مفوضا لإدارة القانون، قد أعلنت أن هدفها، هو ترسيخ افضل الممارسات العالمية، التي تعتمدها في مركز دبي المالي العالمي. كما حرصت على إعلان التزامها،

على مراعاة إرشادات منظمة التنمية والتعاون الاقتصادي، إضافة إلى توجيهات الاتحاد الأوروبي [90].

في هذا السياق، حرصت الإمارات بشكل واضح، على إقرار قانون خاص لحماية البيانات الشخصية، بصيغة تراعي التوصيات الدولية، لاسيما منها تلك الصادرة عن الاتحاد الأوروبي، وإرشادات منظمة التنمية والتعاون الاقتصادي، بحيث غطت الحماية، جميع البيانات الشخصية، بما فيها الحساسة، وعملية نقل وتبادل المعلومات عبر الحدود، وفرض عقوبات صارمة ضد إساءة استعمال هذه البيانات. وأوكلت إلى المفوض بإدارة القانون، مراقبة التزام مركز دبي المالي العالمي به، وبأفضل الممارسات الدولية، في مجال حماية البيانات الشخصية، باعتباره مجالا بالغ الحساسية.

التشريع: مستلزماته، مجالاته، وضوابطه

- مستلزمات التشريع

تشكل الأطر القانونية والتنظيمية جزءا أساسيا، من منظومة حماية البيانات الشخصية، لا يمكن الاستغناء عنه، بالرغم من كل الإجراءات التقنية، أو الممارسات الشخصية، التي يمكن أن يلجأ إليها مستخدم تقنيات الاتصالات والمعلومات، لاسيما على مستوى تحديد المسؤوليات، ومنهجيات وأساليب الحماية، وإقرار الموجبات على معالج البيانات، ومستثمرها، أو ناقلها.

ويؤكد هذا الأمر، المنحى الذي اتخذته القواعد الأوروبية الجديدة لحماية البيانات الشخصية، عندما أقرت عددا من الحقوق الجديدة، لصاحب البيانات، وموجبات على المسؤول عن المعالجة والمعالج، تجاوزت ما كان معمولا به، في القوانين

---

[90] - دبي المالي العالمي يصدر قانون حماية البيانات الشخصية
"وقال معالي الدكتور عمر محمد أحمد بن سليمان محافظ مركز دبي المالي العالمي: يعكس إصدار قانون حماية البيانات وتعيين مفوض لإدارته التزام المركز الدائم بأفضل الممارسات العالمية، خاصةً في مجال بالغ الحساسية مثل حماية البيانات. وفي ظل العولمة وسهولة الحصول على البيانات وتداولها، تتضاعف أهمية إرساء نظام فاعل للحماية وفرض إجراءات قانونية صارمة ضد إساءة استخدام البيانات الشخصية. ونحن ملتزمون في مركز دبي المالي العالمي بتطبيق ومواكبة أرقى المعايير في هذا المجال".
http://www.alittihad.ae/details.php?id=91170&y=2007

الأوروبية الوطنية، التي التزمت توصيات العام 1995. كما يؤشر التشريع الجديد، إلى ضرورة مواكبة التطورات التقنية، وأهمية الانسجام بين القوانين، سواء على المستوى الداخلي، بين دول الاتحاد، أم على مستوى علاقات دول الاتحاد، مع الدول الأخرى، لاسيما منها تلك التي تنقل إليها بيانات المواطنين الأوروبيين.

فالحماية القانونية الداخلية إجراء لا بد منه، لكنه يبقى غير كاف، متى خرجت هذه البيانات إلى منطقة تقع خارج سيادة الدولة.

ولأنه يمكن الانطلاق في أية خطوة تشريعية لحماية البيانات الشخصية، من الإرشادات التي وضعتها منظمة الاقتصاد والتنمية، حول حماية الحياة الخاصة، وحركة انتقال هذه البيانات عبر الحدود، لا بد من الإشارة إلى مسألتين بارزتين في الإرشادات، وهما: الشفافية والمسؤولية.

ويقوم مبدأ الشفافية، على تأمين الوسائل الكفيلة بتحديد وجود البيانات الشخصية، وطبيعتها، وأهداف معالجتها، ووجهة استخدامها، كما وبتحديد هوية الحائز على هذه البيانات، والمكان الذي يمارس فيه نشاطه. أما المسؤولية، فتعني: أن يحترم الشخص الذي يحتفظ بالمعلومات، القواعد، والإجراءات، التي تضمن تطبيق الإرشادات. وقد كان لهذه الأخيرة، أثر على القواعد الأوروبية الجديدة، التي اعتمدت عددا من الإجراءات، تستند على مفهومي الشفافية، والالتزام.

» مجالات التشريع

تؤثر البيانات الشخصية، من خلال دورها في حماية الحق في الخصوصية، والحقوق والحريات المرتبطة به، على الحياة اليومية للشخص، وعلى طريقة أدائه، وتفاعله مع أقرانه، ومرؤوسيه، أو مع السلطات العامة.

لذا، يلاحظ الارتباط الوثيق بين الحق في الخصوصية، وحماية البيانات، كما التأثير المباشر لهذه الحماية، في حماية النظام الديمقراطي، والمبادئ التي يقوم عليها، وفي

مقدمها الإقرار بحقوق الإنسان والمواطن. كما يبدو واضحا، تناول التشريع الخاص بالحماية، مجالات: الحريات والحقوق الأساسية، الحق في الأمان وفي الوصول إلى العدالة، إضافة إلى موجب اعتماد تقنيات الحماية، والإجراءات الكفيلة بضمانها، وبعدم تسرب البيانات وانكشافها.

وعليه، لا بد للقوانين من التطرق إلى تنظيم استخدام البيانات في المجالات كافة، الخاص منها، والتجاري، والحكومي، وإقرار عقوبات على استخدامها، والوصول إليها، بطريقة غير قانونية. وهكذا تطاول أحكامها، علاقات الأفراد بالإدارات الحكومية؛ لاسيما منها تلك الخاصة بمكافحة الجريمة، وبالحفاظ على الأمن، ما يجعل القواعد المعتمدة تنشئ الحقوق والموجبات، وتقر مبادئ وأسسا يجب احترامها، منذ لحظة جمع المعلومات، مرورا بمعالجتها، وصولا إلى مرحلة استثمارها، وإزالتها أو محوها، أو اعتماد تقنيات لتشفيرها، وتجهيلها، بحيث يصبح من المتعذر استخدامها، في تحديد هوية الأشخاص، الذين تعود اليهم، وذلك، بعد تأدية الهدف من استخدامها.

وذلك يعني، حماية واحترام الحريات، بشكل مباشر وصريح، والامتناع عن التعرض لأصحاب البيانات، دون وجه حق، وخارج الحالات الاستثنائية التي تقرها القواعد للسماح بالجمع والمعالجة، دون الرجوع إلى أصحاب البيانات، أحياناً.

وفي هذا السياق، يبرز التحدي الأكبر، وهو تحدي إيجاد التوازن بين الحماية، وحقوق وحريات أخرى، منها ما يتعلق بالأفراد الآخرين في المجتمع، وحرياتهم، مثل: حرية التعبير، وحرية تبادل البيانات، والحق في الوصول إلى المعلومات، ومنها ما يتعلق بحقوق المؤسسات التجارية، في إدارة هذه البيانات وجمعها، والإفادة منها في تسيير نشاطها الاعتيادي، وإدارة شؤون العاملين لديها، كما شؤون زبائنها، وحماية حقوقها، ومنها الآخر، ما يتصل بواجبات الدولة في حماية السلامة العامة والأمن القومي، والتي طالما ارتبطت، بجمع المعلومات، وتبادلها، والوصول إليها.

» ضوابط التشريع

كنا قد عرضنا هذه الضوابط، في دراسة أعددناها سابقا، حول أحوال تشريع حماية البيانات في العالم العربي، ولإنها مؤشرات ثابتة، تأكدت أهميتها، مع إقرار القواعد الأوروبية الجديدة لحماية البيانات الشخصية، والتي دخلت حيز التنفيذ في 25 أيار/مايو 2018، فإننا نعيد استعراضها، لننطلق منها في دراستنا المقارنة للقوانين العربية، التي صدرت في هذا المجال.

تفترض حماية البيانات الشخصية، إحاطة شاملة، بكل الآليات التقنية، ووسائل المعالجة، والتصرف بالبيانات، بحيث لا تترك ثغرات، يمكن النفاذ منها، للالتفاف على الهدف المرجو. وعليه، لا بد لكل إطار تشريعي أو تنظيمي، أو إرشاد، وعلى غرار أي نص قانوني آخر، أو إرشاد أو اتفاقية، أن يلحظ الآتي:

الأسباب الموجبة، التي تلحظ فلسفة النص، وأهدافه. التعريفات الضرورية لوضوح النص ومجال تطبيقه. وعليه لا بد هنا من تحديد: البيانات الشخصية، وعمليات المعالجة، والأنظمة أو الآليات التي يتم العمل بموجبها، إضافة إلى الهيئات والأشخاص المسؤولين والمعنيين، لأهمية تحديد المسؤوليات، في هذا المجال.

تحديد الجهات التي يمكنها جمع البيانات الشخصية، دون إذن مسبق، على أن تحدد أهداف هذا الاستثناء بوضوح، وعلى أن ينسجم هذا الاستثناء، مع مقتضيات السلامة العامة، والأمن القومي، وطبيعة بعض النشاطات المهنية الخاصة.

تحديد الشروط التي يمكن على أساسها، الحصول على إذن بمعالجة البيانات الشخصية، ونقلها، وتبادلها، توضح فيه نوعية البيانات التي يمكن معالجتها، أو نقلها، أو تبادلها، كموافقة صاحب البيانات، والمصلحة المبررة والمشروعة، من جمعها.

تحديد البيانات المستثناة، والأسباب المانعة لمعالجتها، إضافة إلى الحالات التي يمكن فيها تجاوز هذا الاستثناء، شرط الانسجام مع فلسفة النص وأهدافه، أي

الحفاظ على حرمة الحياة الشخصية، والحريات الفردية والعامة، والحقوق الأساسية للإنسان، والنصوص القانونية والأحكام، والمصلحة العامة، أو المصلحة الخاصة للشخص المعني، وحرية التعبير.

إقرار حقوق أصحاب البيانات في الوصول إليها، والتدقيق فيها، وطلب تصحيحها أو محوها، أو منع النفاذ إليها. يضاف إلى ذلك، حق الاعتراض على المعالجة، متى توافرت لدى الشخص أسباب مشروعة، أو متى كان هدف المعالجة، أعمالا تجارية، وترويجية.

إنشاء هيئات رقابية، ذات صلاحيات للملاحقة والعقاب، تسهر على التطبيق، وحسن سير آليات التنفيذ، بحيث تضمن جميع حقوق الشخص، صاحب البيانات، لاسيما لناحية حقوقه في مراقبة التصرف ببياناته، وأوجه استخدامها، ودقتها، ومصداقيتها، والأهداف التي تستخدم لأجلها. وتدخل في هذا الإطار، الشكاوى، والمراجعات والاعتراضات.

تنظيم حقوق الجهات المعنية بمعالجة هذه البيانات، سواء أكانت مؤسسات عامة، أم خاصة، أم أشخاصا طبيعيين يستثمرون هذه البيانات، ويديرونها في إطار نشاطهم العلمي، أو التجاري.

تحديد مسؤوليات الجهات المراقبة وموجباتها، لاسيما لجهة الالتزام بسرية البيانات، والحفاظ على سلامتها وعدم انكشافها، أو تسربها، وتلفها، والتلاعب بها.

إقرار الحق في التعويض عن المخالفات المرتكبة، وأصول مراجعات قضائية وإدارية ملائمة، تعزز ممارسة الشخص لحقه في الحفاظ على بياناته الشخصية، ومن خلالها على حريته الشخصية، وحياته الخاصة.

تأمين حماية البيانات الشخصية المنقولة عبر الحدود، إلى بلد أجنبي، بموجب اتفاقات واضحة، تحترم المبادئ العامة للنص الخاص بالحماية، وفلسفته، على أن تلحظ آليات

موافقة وتصريح، لا تعيق تدفق البيانات لأهداف تخدم تطور التجارة الإلكترونية، والمصلحة العامة، والاقتصاد، والأمن.

تشجيع ودعم، تطوير قواعد تعامل سليم، وإرساء أخلاقيات خاصة، تجارية ومهنية، وإدارية، بالتعامل في مجال معالجة البيانات الشخصية، ونقلها، والتصرف بها، تعزز دور الإطار التشريعي والتنظيمي.

وضع آليات مواجهة، للتحديات الجديدة التي تفرضها الحوسبة السحابية، وإنترنت الأشياء، لاسيما على المستويات التالية: تشجيع التزام الشركات بقواعد الحماية والأمن، تحديد مسؤولية المتعاقدين مع مزودي الخدمة الأساسيين، نوعية الخدمة، طبيعة المسؤوليات، مستويات الحماية، نقل البيانات خارج الحدود الوطنية.

في هذا السياق، تظهر القوانين العربية المعتمدة، في مجال حماية البيانات الشخصية بشكل عام، نزعة إلى الالتزام بمفاعيل عضويتها في الأمم المتحدة، وتوقيعها على المواثيق الدولية لحماية الحقوق والحريات الأساسية، على غرار ما ذهب إليه مشروع القانون الجزائري، عندما ذكر صراحة الالتزام بالعهد الدولي المتعلق بالحريات المدنية والسياسية. وكانت نقاشات البرلمان الجزائري، قد اعتبرته لبنة على طريق الإصلاحات التي بوشرت، في مجال الحفاظ على الحريات، والحياة الخاصة للأفراد.

واعتبر القانون المصري، في الأحكام العامة منه، إن حماية البيانات هي أحدى اهم الحريات الشخصية، والحقوق الأساسية للأشخاص الطبيعيين. أما القانون المغربي، فقد اقر الحق بالحماية، من خلال الدستور[91]، وفي القانون انطلاقا من المبدأ القائل بتسخير المعلوماتية في خدمة المواطن، والحرص على منع تحولها إلى أداة، لإفشاء أسرار الحياة الخاصة للمواطنين.

[91] - دستور المغرب: الفصل 24 • الحق في احترام الخصوصية لكل شخص الحق في حماية حياته الخاصة. لا تنتهك حرمة المنزل. ولا يمكن القيام بأي تفتيش إلا وفق الشروط والإجراءات التي ينص عليها القانون. لا تنتهك سرية الاتصالات الشخصية، كيفما كان شكلها. ولا يمكن الترخيص بالاطلاع على مضمونها أو نشرها، كلا أو بعضا، أو باستعمالها ضد أي كان، إلا بأمر قضائي، ووفق الشروط والكيفيات التي ينص عليها القانون.

كما تتفق القوانين العربية، على هدف ضمان وحماية خصوصية البيانات الشخصية، والحياة الخاصة للأفراد، في مواجهة مخاطر المعالجة الرقمية للبيانات، والمخاطر التي يمكن أن تطلاهم، نتيجة الرقابة، والتدخل غير المشروع، وانعكاس هذا الأمر، على حقوقهم الأساسية وحرياتهم الفردية.

أما قانون حماية البيانات الشخصية الإماراتي، الصادر في العام [92]2007، وبالرغم من غياب الأسباب الموجبة، عن النسخة الانجليزية، التي حصلنا عليها، إلا انه أتى بحسب مندرجاته، منسجما إلى أبعد حد، مع التشريع الأوروبي، وبالأخص التوصيات الأوروبية الصادرة في العام 1995، وقد عكس برأي المسؤولين في الإمارات، رغبة في التزام افضل الممارسات العالمية، وتطبيق أرقى المعايير، في مجال الحماية.

[92] - https://www.difc.ae/files/7814/5517/4119/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf

﴿ الفصل الثاني ﴾

بين القوانين العربية والنصوص الدولية

انطلاقاً من الضوابط التي ذكرناها آنفا، وبالاستناد إلى الأطر الدولية، المعمول بها، نعرض للحماية في القوانين العربية، لاستشفاف أوجه الشبه والاختلاف، فيما بينها، من جهة، وبينها وبين القوانين الدولية، والأوروبية بشكل خاص، من جهة ثانية. كما سنحاول إلقاء الضوء على النواقص التي تعتريها، تمهيدا لاستطلاع الخطوات، التي يمكن أن تساهم في معالجتها، بما يحقق الغايات المرجوة من اعتمادها.

وقبل التطرق إلى تفاصيل المبادئ، والحقوق، والموجبات، وحماية البيانات، لا بد من الإشارة إلى أن اعتماد المبادئ، أو الأحكام ذاتها، على مستوى التشريع، لا يعني بالضرورة، حماية متشابهة، حيث يمكن أن يختلف الأمر على مستوى التنفيذ.

إذ قد يقرر القانون استثناء بعض عمليات المعالجة، لأسباب تتعلق بالسلامة العامة، فيما يختلف تفسير هذه الأخيرة، بين بلد وآخر، أو كأن يقرر شرعية جمع البيانات، استنادا إلى مجرد عدم رفض المستخدم لعرض ما، واعتبار هذه العملية شرعية، إلى أن يقرر صاحبه البيانات، طلب محوها، بينما لا تقر شرعية عملية الجمع في بلد آخر، إلا متى بادر الشخص المعني، إلى إعطاء موافقة صريحة، على جمع بياناته، تتمثل في مبادرة إيجابية من قبله، كإرسال طلب تسجيل في الخدمة، أو في العرض المقدم، مع تأكيد بعض المعلومات، وتفعيل الحساب، بعد إتمام عملية التسجيل.

وتستوقفنا هنا، مسألة خلافية أخرى، على مستوى تفسير ما يعتمد من مفاهيم مطاطة، وعامة، مثل: "المناسبة والضرورية"، لاسيما بعد الإشكالات، التي أثارتها الفضائح الأخيرة، حول الرقابة الشاملة، التي تقوم بها بعض الدول، على المواطنين

والأجانب، تحت شعار، مكافحة الجرائم الخطيرة، والإرهاب، وحماية الأمن القومي.

يضاف إلى ذلك، حقيقة ما نعرفه، عن صعوبة التوصل إلى اتفاق، بين الدول، على تفسيرات نصوص الاتفاقيات الدولية، كما بدا واضحا حتى الآن، في مجال حقوق الإنسان والمواطن، والحريات المدنية، والسياسية.

وفي هذا السياق، لا بد وان تبرز مسألة حماية البيانات الشخصية، بعد عبورها النطاق الوطني، لاسيما وان الحماية يمكن أن تفقد هدفها الأساسي، في مواجهة تحديات الأبعاد الدولية للحفاظ على الحياة الخاصة، كحق من حقوق الإنسان الأساسية.

التعريفات

- التعريف والأمن القانوني

يعتبر التعريف عنصرا من العناصر المؤسسة للأمن القانوني، من حيث تحديده للمفاهيم القانونية، ومحتوى الالتزامات والحقوق، والأفعال الجرمية، وغير ذلك، مما يلجأ إليه في تطبيق القانون. ويستند الأمن القانوني، فيما يستند، إلى وضوح المفاهيم، وحدود التطبيق، ومجالاته، لأية قاعدة قانونية.

من هنا، يعتبر الإطاران التشريعي والتنظيمي المناسبان لنتائج الأعمال القانونية؛ كالعقود، أو غير القانونية؛ كالأفعال الجرمية وغير الجرمية، حاجة ملحة، في استقرار العلاقات، ومصداقية التعاملات في المجتمع، لاسيما في معرض معالجة الخلافات والنزاعات، التي يمكن أن تنشأ، نتيجة لها.

ويعتبر التعريف، في هذا السياق، مانعا إلى حد بعيد، لتضارب الأحكام، وضامنا لتطبيق التشريع بشكل عادل وسوي، فضلا عما يوفره من اطمئنان للمواطن، بشكل خاص، والفرد بشكل عام، إلى وجود قاعدة قانونية واضحة، تبنى على مفاهيم محددة، يستطيع اللجوء إليها كإطار يضمن حمايته.

وبالرجوع إلى عناوين قوانين حماية البيانات الشخصة، وإلى الأسباب الموجبة لإقرارها، تطالعنا مفاهيم أساسية، حاضرة كمفاتيح دالة، على المحور الذي تحاك حوله القواعد القانونية، والمسؤوليات، والحقوق، والموجبات، والمبادئ، وآليات التطبيق.

وقد عرفت قوانين حماية البيانات الشخصية العربية، المفاهيم التي رأت ضرورة تحديدها، بسبب ورودها في نصوص القانون، فاتفقت جميعها على تحديد الجهات المقصودة، أي صاحبة السلطة، والمولجة اتخاذ القرار، والتي يفترض الرجوع إليها؛ سواء أكان ذلك، لمراجعة بخصوص مخالفة، أو للحصول على إذن ما، أو تصريح بالمعالجة، كالوزير، والوزارة، والإدارة، والجهة المختصة، وسلطة الحماية.

وفيما أعطت جميعها تحديدا للبيانات الشخصية، والمسؤول عن المعالجة، ومعالجة البيانات الشخصية، والمعالج، والشخص الطبيعي، لم يلحظ بعضها تعريف مفاهيم لا تقل أهمية، أقله، لدورها في إرشاد الجهات المعنية، بالالتزام بالقواعد القانونية، من خلال توضيح نطاق الحماية، والحقوق، والموجبات.

ويأتي في عداد المفاهيم التي سقطت، من بعض القوانين، البيانات الحساسة، والوراثية، والجينية، والطبية، علما أن الاستخدام السيئ لنتائج معالجة هذه البيانات، أو حتى لمعالجتها بكل بساطة، يمكن أن يكون ذا أثر شديد السلبية، على الحق في الخصوصية، الذي يبرز في عناوين، وأحكام، وأهداف القوانين، إضافة إلى إمكانيه مسه بالحقوق الأساسية، التي تضمنتها الشرع الدولية لحقوق الإنسان، وليس اقلها، التمييز على أساس الانتماء العرقي، أو لأسباب صحية، ووراثية.

بالمقابل، أضافت بعض القوانين، المصطلحات، التي بدت ضرورتها للمشترع، في سياق تحديد الآفاق التقنية، لحركة البيانات وعملية معالجتها. فقد عرف كل من التشريع القطري والمصري، التسويق المباشر، والاتصال الإلكتروني، وإنشاء

الاتصال الإلكتروني، ومشغل الموقع الإلكتروني، دون أن يقدم هذا الأمر، قيمة مضافة، على أطر الحماية القانونية المعمول بها، لاسيما وان القانونين، قد حرصا على أن يشملا كل أساليب وطرق المعالجة، حتى اليدوية منها، لدى تحديد نطاق القانون [93].

وفي السياق عينه، لم يشكل غياب هذه المفاهيم، برأينا، أي انتقاص، من وضوح الأطر التطبيقية لأحكام القانون التونسي، والمغربي، والموريتاني. علما أن هذا الأخير، كان الوحيد، الذي تطرق إلى تعريف مدونة السلوك، التي يفترض بالمسؤول عن المعالجة إعدادها.

وعليه، لا بد بداية، من التوقف، عند التعريفات البارزة، في قوانين حماية البيانات الشخصية، بشكل عام، وفي القوانين العربية، بشكل خاص.

- **تعريف البيانات الشخصية**

قبل الدخول في تفاصيل أحكام الحقوق والالتزامات، والآليات الخاصة بالتنفيذ والرقابة، والأشخاص المعنيين، وموجبات معالجي البيانات والمسؤولين عن المعالجة، من الضروري تعميق مفهوم البيانات الشخصية، بشكل خاص، لأنها تشكل محور تشريع الحماية، الذي تبنى حوله كامل منظومة الحماية، وتوزع المسؤوليات، وتحدد على أساسه هذه الأخيرة، بناء على العلاقة بعملية معالجتها، إضافة إلى تأثير هذا التعريف، في بناء مدلول المفاهيم الأخرى.

» **مهمة معقدة**

لتطبيق القانون، والموجبات التي يفرضها، بشكل سليم، ولتقرير العقوبات، في حال عدم احترام قواعد ومبادئ حماية البيانات الشخصية، لا بد من تحديد

[93] - مادة (٢) من القانون القطري رقم 13 لسنة 2016 - تسري أحكام هذا القانون على البيانات الشخصية عندما تتم معالجتها على نحو إلكتروني، أو يتم الحصول عليها أو جمعها أو استخراجها على أي نحو آخر تمهيداً لمعالجتها إلكترونياً، أو تتم معالجتها عن طريق الجمع بين المعالجة الإلكترونية والمعالجة التقليدية.

هذه البيانات، بشكل واضح ودقيق. ويعتبر هذا الأمر، من التحديات التي تواجه الأجهزة المعنية بالرقابة، على حسن الالتزام بالأحكام القانونية، كما تساعد الأجهزة القضائية، في معرض تطبيقها القواعد القانونية، وتساهم في مساعدة الشركات، أو الجهات العاملة في مجال جمع البيانات ومعالجتها، على اتخاذ القرارات بشأن الإجراءات، والتدابير المفترض اعتمادها.

لكن هذه المسألة، ليست بالبساطة التي يمكن أن تبدو عليها، للوهلة الأولى. فبعض خصائص الأنظمة المعلوماتية، يمكن أن تجعل هذه المهمة، شديدة الصعوبة، بسبب حجمها وتعقيداتها، والطريقة التي تعتمدها في فرز البيانات الشخصية التي تعالجها. يضاف إلى ذلك، التطورات التقنية والإدارية المستمرة، والتي تتوالى دون انقطاع، ويزاد عليها، دخول أشخاص غرباء، من خلال العقود، التي يمكن أن تلجأ إليها الشركات المسؤولة عن المعالجة، لتنفيذ عمليات المعالجة، جزئيا، أو كليا.

علاوة على ذلك، لم تعد الأنظمة المعلوماتية، أنظمة داخلية مقفلة، بل إنها، تحولت إلى التفاعلية التي تفسح في المجال أمام تبادل الآراء، والمعلومات، والبيانات، بين عدد كبير من الجهات، كالزبائن، والشركاء، وعموم مستخدمي الإنترنت، ما يجعل مهمة تحديد البيانات الشخصية، مهمة تستوجب تقاطع عدد من المصادر، ومراجعة أساليب العمل، والأنظمة، والتطبيقات.

ويفرض هذا الأمر، مقاربة ومنهجية جديتين، تسمحان بتطبيق قواعد الحماية، بشكل فاعل. فالنصوص التي تقرر الحماية، تنظم طريقة المعالجة، أيضاً. ومن هنا، تكون المسألة، ليس فقط في تحديد البيانات المعرّفة شخصية، بل أيضاً، في تحديد عملية المعالجة، لاسيما وان الأمرين مرتبطان بشكل عضوي. وغالبا ما يمكن التعرف على عمليات المعالجة المرافقة للبيانات، من خلال تحديد هذه الأخيرة، والعكس صحيح. فالعودة إلى مسار المعالجة، يمكن أن تكشف البيانات التي تم

جمعها،وحفظها، والتي ربما لا يمكن أن تظهر، بطريقة أخرى.

من هنا، يفترض بالمسؤول عن معالجة البيانات، والذي يحاول تحديد البيانات الشخصية، أن ينتبه إلى قدرة هذه البيانات، وطرق معالجتها، على تحديد الشخص الطبيعي، الذي تعود إليه. وترتبط صحة الجواب هنا، حول اعتبار البيانات شخصية أم لا، بمدى شمولية نظرة هذا الشخص، ومعرفته بالمعالجات التي تتم على المعلومات، إضافة إلى قدرته على تصور، وتوقع إمكانات سوء الاستخدام. ويمكن أن ينتج هذا الأمر، مثلا، عن التحول عن أهداف المعالجة، وغاياتها. وهذا ما يجعل تحديد البيانات الشخصية، خارج إطار البيانات الاسمية (اسم الشخص، واسم عائلته، ...)، أمراً صعبا، يفترض جهدا ملحوظا، من قبل المعنيين بالمعالجة.

وإذا أضفنا على ما تقدم، ضرورة مواكبة التطورات التقنية، وحاجات المستخدمين أو الزبائن إلى خدمات جديدة، تبرز تحديات جديدة، وصعوبات أخرى، نتيجة المعالجات الجديدة، ذات الأهداف المغايرة، للمعالجات الأولى.

والمثال الأوضح هنا، هو تقنيات البيانات الضخمة، التي تتيح معالجة كميات هائلة من البيانات والمعلومات، لاستخراج القيمة المضافة، التي يمكن أن تستفيد منها الشركات. فمع هذه الإمكانات غير المحدودة، لا يمكن الحديث عن نظرة شمولية مسبقة، لكل المعالجات التي يمكن أن تتم على المعلومات، ما يجعل مواكبة تطور عملية معالجة المعلومات، مهمة دقيقة، في بيئة تقنية متحولة، وسريعة التطور، تحفل بالتغيرات الدائمة.

من جهته، يزيد اللجوء إلى خدمات مزودي خدمات، خارجين عن إطار المؤسسة التي تتولى معالجة البيانات، الأمور تعقيدا، لناحية تحديد البيانات الشخصية، لاسيما وان هذا الأمر، يفترض تحديد الشركاء، وعمليات المعالجة التي تطال المعلومات، وتبادل البيانات والمعلومات الشخصية، وإدارة العقود التي ترعى هذه العلاقة،

وتحديد الموجبات والالتزامات. فليس من السهولة بمكان، تحديد الشركاء، أو الجهات التي تنتقل إليها المعلومات، في عالم الحوسبة السحابية، وعقود الخدمات التي تعقد عملية تحديد البيانات الشخصية، في نطاق مزودي الخدمات.

من هنا، تبقى افضل الممارسات التي تساعد على تحديد هذه المعلومات، هي تلك التي تجمع بين الرؤيتين، الإدارية والتقنية، بحيث لا تتصل فقط بالبيانات المسجلة، وإنما أيضاً بحركة تدفقها، وبعمليات المعالجة. وفي هذا الإطار، يمكن أن يلجأ إلى تصنيف الأشخاص الطبيعيين الذين يتعاملون مع المؤسسة، وتحديد فئات البيانات التي تجمع من قبل كل منهم، إضافة إلى تحديد مسارات تدفق البيانات وتبادلها، من نقطة جمعها إلى نقاط معالجتها المختلفة، بما يسمح بمعرفة كل العمليات التي تخضع لها، ليصار بعدها إلى معرفة إمكانات التعرف إلى الأشخاص المعنيين، سواء من خلال المعلومات، أو من خلال أساليب المعالجة. فإذا سمح ذلك بتحديد الأشخاص، كانت هذه البيانات والمعالجات شخصية.

» بين البيانات الشخصية والبيانات ذات الطابع الشخصي

من المهم في أي تعريف لمصطلح ما، أو لمفهوم قانوني، يحدد على أساسه، نطاق القانون، أن يكون دقيقا، واضحا، ومحددا، منعا لأي تجاوز، أو إساءة لاستخدامه، في اكتساب حقوق غير مشروعة، أو في الاعتداء على حقوق مشروعة. انطلاقا من هذا المبدأ، سنقوم باستعراض التعريفات التي اعتمدت في القوانين العربية، ومقارنتها بما هو معتمد على المستوى الدولي، لاسيما الأوروبي منه، لتبيان مدى تقاربها وتباعدها، وتقدير فاعلية اللجوء إليها، كأساس في الحماية.

وقد عرفت النسخة الأولى من الإرشادات، التي أصدرتها منظمة التعاون الاقتصادي والتنمية، في العام 1980، البيانات الشخصية، على الشكل التالي: "تعتبر البيانات الشخصية، كل معلومة عائدة لشخص طبيعي محدد، أو قابل

للتحديد"[94].وعليه، فهي تلك البيانات، التي تنقل معلومات، يمكن ربطها بشخص معين، لتحديد هويته.

إلا أن هذا التعريف أثار بعض الإشكالات، إذ استثنى بيانات، يمكنها هي الأخرى، أن تساعد على تحديد هوية الشخص، أو تعقبه وملاحقته، عبر سماحها بتحديد هويته، بشكل غير مباشر، وان لم تكن مرتبطة بهويته الشخصية. وترد في هذا السياق، البيانات التي لا تعود إلى الشخص الطبيعي، وإنما إلى وسيلة يستعملها: كرقم تسجيل السيارة، ورقم الهاتف الثابت والنقال، أو المعلومة المرتبطة، بأية وسيلة أخرى يحملها.

وتكمن خطورة استثناء هذه الفئة من البيانات، أو بقائها خارج نطاق القانون، في الإمكانية التي تتيحها، بالتعدي على خصوصية الأشخاص، دون رادع، من خلال معالجة البيانات، بعيدا عن أعين أجهزة الرقابة، والأشخاص المعنيين، نظرا لعدم إمكانية تطبيق النص، الذي يستبعدها، بطريقة غير مباشرة.

وبحسب القوانين المعتمدة في هذا المجال، ولكي تتم معرفة متى، أو كيف يكون الشخص قابلا للتعريف، يجب أن تؤخذ بعين الاعتبار، جميع الوسائل المتاحة والممكنة، لتحديد الهوية، والتي يمكن أن يحصل عليها المسؤول عن المعالجة، أو أي شخص آخر، يمكن أن يصل إليها.

من جهته، نص التشريع الفرنسي الذي صدر في العام 1978، على حماية المعلومات الاسمية، حاصرا بذلك، نطاق تطبيقه بشكل دقيق، في كل معلومة تشير إلى هوية الشخص، من دون أي التباس. إلا أن هذا القانون، جرى تعديله في

[94] - PART ONE. GENERAL DEFINITIONS. For the purposes of these Guidelines: a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;b) "personal data" means any information relating to an identified or identifiable individual (data subject);c) "transborder flows of personal data" means movements of personal data across national borders. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1

العام [95]2004، مجاراة للتحولات التقنية، التي جعلت انكشاف الهوية، وتحديد الشخص ممكنا، باللجوء إلى تقنيات وبرمجيات، تعمل على تقاطع المعلومات، وتحليلها. وهكذا، توسع نطاق تطبيق القانون الفرنسي، باعتماد عبارة "المعلومات ذات الطابع الشخصي" بما مهد لحماية بيانات غير اسمية[96]، فاتحا بذلك المجال أمام حماية أوسع، ولكن أمام التباسات أكبر، أيضا.

وبالفعل، فقد اعترضت لجنة المعلوماتية والحريات في فرنسا، على الاجتهاد[97]، الذي اعتبر في قرارين متتاليين، صادرين عن محكمة الاستئناف في باريس، أن العنوان الخاص برقم التعريف الإلكتروني للجهاز IP[98]، ليس من البيانات الشخصية، كونه يسمح بتحديد هوية الجهاز، لا هوية الشخص الذي يستعمله. وفي ذلك، بحسب رأي اللجنة، خطر يفتح الباب للتعديات على الخصوصية، من خلال جمع هذه البيانات، من دون الحصول على الترخيص المسبق، والمفروض قانونا، لكل ما يدخل في نطاق تعريف البيانات الشخصية.

في هذا السياق، اتخذت المحكمة الأوروبية لحقوق الإنسان، موقفا من اعتماد تعريف واسع للبيانات الشخصية، التي يمكنها أن تعرض الحياة الخاصة للانكشاف، في عدد من قراراتها، وذلك بالرغم من أن مفهوم الحياة الخاصة، لم يكن قد اتخذ بعده العالمي، بعد.

[95] - Loi 801 intitulée «loi pour la confiance dans l'économie numérique» du 21 juin 2004

[96] - La loi du 6 janvier 1978 "informatique et libertés" visait les informations nominatives. La loi du 6 août 2004 remplace le terme "information nominative" par celui de "donnée à caractère personnelle".

[97] - CA Paris, 27 Avril 2007 :" "L'adresse IP ne permet pas d'identifier le ou les personnes, qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur.". Et CA Paris, 15 Mai 2007 :» "Que cette série de chiffre en effet ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon".

[98] - L'adresse IP est le numéro qui permet d'identifier chaque ordinateur sur le réseau Internet. Elle se décompose dans version 4 en une série de 4 nombres allant de 0 à 255.

فاعتبرت في قرار صادر عنها، في العام 2000[99]، أن الحياة المهنية، تكون مشمولة في بعض الأحيان، بالمادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان، التي تحمي الحياة الخاصة. واستلهمت المحكمة، الاتفاقية الأوروبية رقم 108، حول حماية الأشخاص من المعالجة الإلكترونية لبياناتهم الشخصية، مذكرة بانها تهدف إلى حماية أية معلومة تخص شخصا معرفا، أو قابلا للتعريف.

وكانت هذه القضية، قد حولت إلى المحكمة، في العام 1998، بعد اعتراض احد المواطنين السويسريين، على استعمال الأحرف الأولى من اسمه، في ملف جمعته أجهزة الأمن، لان في ذلك خطر انكشاف هويته. وكانت البيانات المدونة، تشير إلى واحدة من مخابراته الهاتفية المهنية، مع إحدى زبوناته، والتي كانت تعمل في حينها، لدى السفارة الروسية، في زوريخ.

اعتمدت محكمة العدل الأوروبية هذا الاتجاه، كمرجع لتوضيح التعريف الوارد في الإرشادات الأوروبية، معتبرة إياه شاملا العنوان الخاص برقم التعريف الإلكتروني للجهاز IP، وسجلات الحضور إلى العمل، وبيانات أجهزة الرقابة، لاسيما منها التصويرية، وكل البيانات التعريفية الخاصة بالاتصالات. إلا أنها أضافت إلى ذلك، شرطا يتعلق بإمكانية حيازة الجهة التي تملك المعلومة، لوسائل شرعية، تمكنها

[99] - CEDH 16 Fevrier 2000, "Amann contre Suisse" Req. 27798/95 que le terme « vie privée » ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables ; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de « vie privée »
66. En l'espèce, la Cour relève qu'une fiche a été établie concernant le requérant, sur laquelle il a été indiqué que ce dernier était un « contact auprès de l'ambassade russe » et faisait « du commerce de différentes sortes avec la société [A.] 67. Pour la Cour, il s'agit là sans contredit de données relatives à la « vie privée » du requérant et l'article 8 trouve en conséquence à s'appliquer à ce grief également
https://www.doctrine.fr/d/CEDH/HFJUD/GRANDCHAMBER/2000/CEDH001-62971

من تحديد هذه الهوية[100].

ويتناسب هذا التوسع في التعريف، مع قانون يهدف إلى توفير حماية فاعلة، وتأمين معدل أعلى من الثقة. بالإضافة إلى ذلك، يستجيب هذا التعريف، لحاجة مركزية: إلا وهي بناء الثقة والأمان في الفضاء السيبراني، من جهة أولى، و مواكبة التطورات المتسارعة، في مجال تقنيات المعلومات، من جهة أخرى، حيث لم يعد ممكنا، توقع المدى الذي تبلغه قدرات تكنولوجيا معالجة المعلومات، ولا نتائج الجمع بين تقنيات مختلفة ومتنوعة، سواء على حرمة الحياة الشخصية، أوعلى أمن الدول، التي تجمع وتعالج وتتبادل، البيانات الشخصية.

وإذا كان هذا التعريف ملائما، برأينا، ومتناسبا مع الاتجاهات الدولية، وحاجات الحماية، ووسائل البحث عن البيانات والمقارنة بينها، إلا انه يقتضي الانتباه، إلى الاختلاف بين مفهومي البيانات والمعلومات. وعلى سبيل تبسيط الأمر، دون التعمق فيه، فالمعلومة، هي ما ينتج عن معالجة البيانات، وتنظيمها، وتحليلها، بينما البيانات أي الداتا Data، هي المعلومات الخام، التي لم تتم معالجتها[101].

وبالرجوع إلى حيثيات، ومقدمات القوانين، نلاحظ توافقا على اعتبارها موجهة نحو حماية الأشخاص الطبيعيين، على غرار القوانين الأوروبية، والاتفاقيات الدولية في هذا المجال. كما نسجل، اعتبار البعض منها، كالقانون التونسي[102]، والمصري،

[100] - CJUE 19 octobre 2016 "Breyer contre Allemagne" Aff. C-582/14
L'article 2, sous a), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doit être interprété en ce sens qu'une adresse de protocole Internet dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne
http://curia.europa.eu/juris/document/document.jsf?docid=184668

[101] - Data vs. Information Diffen English Language Grammar Words
There is a subtle difference between data and information. Data are the facts or details from which information is derived. Individual pieces of data are rarely useful alone. For data to become information, data needs to be put into context.
https://www.diffen.com/difference/Data_vs_Information

[102] - الباب الأول . أحكام عامة الفصل الأول لكل شخص الحق في حماية المعطيات الشخصية المتعلقة بحياته الخاصة باعتبارها من الحقوق الأساسية المضمونة بالدستور

وذلك في مطلع القانون، الحق في حماية البيانات الشخصية، من الحقوق الأساسية للإنسان، مما يؤمن حماية قوية للبيانات، بغض النظر عن حماية الحق في الخصوصية.

» في القوانين العربية: تعريف واسع

يسجل ميل في جميع القوانين العربية، إلى التعريف الواسع للبيانات الشخصية. ولهذه الغاية، لحظت جميعها مادة خاصة بتعريفها، باعتبارها عنصرا أساسا، في تحديد نطاق تطبيق القانون. إلا إنها اختلفت من حيث المصطلحات المستخدمة في التعريف، فمنها من اعتمد مصطلح البيانات الشخصية؛ كتونس وقطر والجزائر، ومنها من اعتمد مصطلح البيانات ذات الطابع الشخصي؛ كالمغرب، ومنها من عرف البيانات الشخصية، بمصطلح "البيانات ذات الطابع الشخصي" كمصر.

ويتسم التعريف المعتمد في جميع القوانين العربية، بميل إلى تأمين حماية فاعلة، باستخدام تعابير ومصطلحات واسعة المدلول، تخدم هذه الغاية، ويمكنها تغطية مروحة واسعة من البيانات. فقد ذكر المشترع التونسي "كل البيانات"، بغض النظر عن مصدرها أو شكلها، بمجرد إنها تساعد على تعريف الشخص الطبيعي، أو على جعله قابلا للتعريف، سواء كان ذلك بصورة مباشرة أم غير مباشرة، مع استثناء المعلومات المتصلة بالحياة العامة، أو المعتبرة كذلك قانونا.

وكذلك فعل كل من المشرع المغربي، والمصري، والقطري، والموريتاني، عندما تحدث عن أية معلومة، بغض النظر عن دعامتها، ومصدرها، ونوعها.

وبالمقارنة مع القوانين والتوصيات المعمول بها دوليا، يعتبر هذا التعريف، مواكبا للتحولات التقنية، التي تجمع أنواعاً من البيانات، تنتج عن تقاطع المعلومات، ومقارنتها، لاسيما وانه قد لحظ التعريف المباشر، أو غير المباشر، عبر البيانات، أو عبر الجمع بينها، وبين أية بيانات أخرى.

- البيانات الحساسة

البيانات الحساسة، هي فئة من البيانات الشخصية، ذات نطاق أضيق من نطاق البيانات الشخصية، بشكل عام. لكن غالبية القوانين، تحظر جمعها، نظرا لارتباطها المباشر، بحقوق إنسانية، وحريات أساسية، تقرها مواثيق دولية، وقوانين أساسية، كالدساتير. فهذه البيانات، بحسب التعريف الذي اعطي لها، كل معلومة تكشف العرق، والأثنية، والمعتقدات الفلسفية والدينية، والآراء السياسية، والنشاطات النقابية، والصحة، والحياة الجنسية. وبذلك، ترتبط هذه البيانات، بحرية المعتقد، ومنع التمييز، وحرية الرأي.

وتظهر القواعد الخاصة بتنظيم حماية هذه البيانات، في المبادئ والاستثناءات، الواردة في قوانين الحماية. والمبدأ العام، هو حظر معالجتها، إلا من قبل إدارات الدولة المختصة، وضمن اطر القوانين المرعية الإجراء.

وهنا تجدر الإشارة، إلى إمكانية تعريف فئات البيانات الحساسة، بشكل مختلف في القانون، نظرا إلى الاختلافات التقليدية بين الأنظمة القانونية. والنتيجة الحتمية لهذا الأمر، ستكون تباينات على مستوى التشريع، أو على مستوى الإطار التنظيمي الذي يختص بحظر معالجتها، أو السماح بها.

يضاف إلى ذلك، صعوبة إيجاد توافق عالمي، على تحديد فئات من البيانات، التي تعتبر حساسة. ولذلك، نلاحظ أن الإرشادات التي أقرتها منظمة التعاون الاقتصادي والتنمية، قد بقيت في إطار التنظيم العام، حين نصت على ضرورة إيجاد أطر مناسبة، تمنع معالجة بعض فئات البيانات الشخصية.

وكانت القواعد الأوروبية الجديدة، قد تركت للدول عملية تنظيم معالجة "البيانات الحساسة"، على ما جاء في الفقرة العاشرة، من ديباجة التشريع[103]، حرية

[103] - 10 " Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées «données sensibles»).

تنظيم شروط الحظر، أو السماح، بمعالجة البيانات الحساسة، دون الخروج، عن التزاماتها، بأحكام التشريع الأوروبي، حيث نصت المادة التاسعة[104]، على حظر معالجة البيانات الشخصية، التي تكشف الأساس العرقي، أو الإثني، والآراء السياسية، والمعتقدات الدينية، والفلسفية، والانتماء النقابي، والبيانات الجينية، والبيومترية، بهدف تحديد هوية شخص طبيعي بذاته، كما حظرت معالجة البيانات الصحية، أو الجنسية. وهذا يعني، عمليا، التزام دول الاتحاد الأوروبي، باعتبار جميع البيانات المذكورة صراحة، في المادة التاسعة، بيانات حساسة.

لكن الحماية المشددة لهذه البيانات، يمكن أن تسقط، في عدد من الحالات، ولأسباب يحددها القانون، وتتوزع بين ما هو مرتبط بفائدة الشخص المعني، وبتصرفه الإرادي، من جهة أولى، وبين ما هو مرتبط بمصالح، أو بالتزامات وقيم، تتعدى نطاق حماية الفرد، إلى حماية المجتمع، من جهة ثانية.

وهكذا، تخرج البيانات الحساسة، عن نطاق حظر المعالجة، في سياق تطبيق مبدأي: سلطان الإرادة الفردية، أي موافقة الشخص المعني، والمصلحة العليا للبلاد. وتبقى هذه الحالة الأخيرة، مشروطة بحسب العديد من الأنظمة القانونية، بالحصول على إذن خاص، يصدر بمرسوم، أو بغيره من الأوامر الإدارية.

كما يمكن أن يسقط الحظر، عندما يختار الشخص المعني، الانضمام إلى تجمعات دينية، أو سياسية، أو نقابية، تعالج البيانات الحساسة للمنتسبين إليها، وذلك تحت شعار: الحق في الاختيار. ولا تتمتع سلطة الحماية، بأية حق في الرقابة، على عمليات المعالجة هذه، انطلاقا من مبدأ احترام الحرية الدينية، وحرية التجمع، والمخاطرة الطوعية، التي يتحملها المنتسب، بعد أن يزن بوعي، المصالح، والمخاطر المختلفة، التي

---

[104] - Art. 9 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

تترتب على خياره.

كما يمكن لهذه البيانات، أن تفقد امتياز الحماية المشددة، التي تتمتع بها، في مقابل قيم أكبر وأهم، كالمصلحة العامة، والصحة العامة، والمصلحة العلمية.

وفي الولايات المتحدة الأميركية، يمكن أن تضاف إلى هذه الفئة، عنوان الجهاز الإلكتروني[105]، والبيانات المالية، وبطاقة الضمان، وبيانات الأطفال.

على المستوى العربي، حرص جميع المشرعين العرب، على غرار ما ذهب إليه المشرعون، حول العالم، على إبراز تعريف خاص بالبيانات الحساسة، سواء من خلال المادة المخصصة لتعريف البيانات الشخصية، أو من خلال تعريف منفصل. وقد شملت هذه البيانات، من حيث التعداد، الخصائص الفيزيولوجية، والجينية، والبيومترية، والعرقية، والإثنية، والقناعات الفلسفية والدينية، والسياسية، والثقافية، والاجتماعية.

وقد افرد كل من المشرع القطري، والمصري، فصلا خاصا، بالبيانات الشخصية ذات الطبيعة الخاصة، حيث سرد عددا من البيانات، التي ترد ضمن فئة البيانات الحساسة، مضيفا البيانات المتعلقة بالأطفال، والصحة، والعلاقة الزوجية، والجرائم الجنائية.

في المقابل، أتاح المشرع القطري، إمكانية إضافة أنواع جديدة من البيانات ذات الطبيعة الخاصة، بقرار من الوزير المختص، إذا كان من شأن سوء استخدامها، أو إفشائها، الحاق ضرر جسيم بالفرد. كما اعطي الوزير صلاحية فرض احتياطات إضافية، لحماية هذا النوع من البيانات. أما المشترع المصري، فقد أعطى هذه الإمكانية، لجهاز حماية البيانات.

[105] - i Privacy and data protection legislation and standards - The United States has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk: a. Financial, insurance and medical information; - b. information about children and students; c. Telephone, internet and other electronic communications and records; d. Credit and consumer reports and background investigations at the federal level; https://thelawreviews.co.uk/chapter/1151376/united-states

وقد حظر التشريع التونسي، معالجة هذه البيانات، فعرضها مفصلة في المادة 14، في إطار البيانات التي يحظر معالجتها، دون أن يخصصها بتعريف. وكذلك فعل التشريع المصري، في الباب الثالث، والقطري في الفصل الرابع، وذلك، تحت عنوان: "البيانات الشخصية ذات الطبيعة الخاصة"، بينما عرفها القانونان الموريتاني[106]، والمغربي[107].

- **البيانات الصحية**

يعتبر تعريف هذه البيانات، بشكل خاص، شديد الأهمية، نظرا لارتباطها الحميم بخصوصية كل شخص طبيعي، إذ لا يمكن الكشف عنها، إلا لمن يمكن للشخص ان يثق به، ولغاية الحصول على مساعدة، في مواجهة وضع صحي، أو حالة مزعجة. وهي شديدة الارتباط بسلامته الجسدية، وربما النفسية، والعقلية أيضا، ويمكنها ان تكون سببا مؤثرا، وبشكل مباشر ودراماتيكي، على مستقبله المهني، وحالته العائلية، أو الاجتماعية. من هنا، يفهم حرص المشترع، كما حرص النقابات المهنية، على وضع أحكام قانونية، ومدونات سلوك خاصة، بحمايتها.

فالبيانات الصحية، هي جميع البيانات الطبية، الخاصة بوصف حالة المرض، وظروفه، وعلاجاته، ومسار الشفاء، وغير ذلك، مما يتعلق بمسيرة المرض والمريض. وقد حرصت جميع الأنظمة القانونية، على إخضاعها للحماية، من خلال السرية المهنية، أي مبدأ "السرية الطبية".

ويعتمد هذا المبدأ، في إطار الأخلاقيات الطبية، التي ترعى العلاقة بين المريض وطبيبه، حيث يمكن لهذا الأخير، أن يطلع خلالها، على أمور صحية، وشخصية، وربما مهنية خاصة بالمريض، وهو ملزم بالحفاظ على سريتها، دون تمييز، بين ما يكتشفه شخصيا، أو بين ما يبوح به المريض، من تلقاء ذاته.

[106] - موريتانيا: 7 - البيانات الحساسة: أي معلومة تتعلق بالرأي، أو الأنشطة الدينية، أو الفلسفية، أو السياسية، أو النقابية، أو الحياة الجنسية، أو العرق، أو الصحة، أو التدابير الاجتماعية أو المتابعة القضائية، أو العقوبات الجزائية، أو الإدارية.

[107] - المغرب: -3 معطيات حساسة: معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية، أو القناعات الدينية والفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما في ذلك المعطيات الجينية.

وقد جرى تطوير هذا المفهوم القديم، نظرا لأهميته، في الحفاظ على حقوق المريض، ومصداقية المهنة، في القرن الماضي، في سياق أخلاقيات المهن الطبية، وحقوق المريض. ويبنى التزام الطبيب بالسرية، على مبدأ توقعات المريض، أي الثقة، والأمانة، وحفظ حقه في الخصوصية. أما إطاره القانوني المباشر، فهو العلاقة التعاقدية، التي تنشأ بينه وبين المريض.

إلا أن هذا السر، يفقد ميزة حمايته، متى تعلق الأمر، بالتزام قانوني، يفرض على الطبيب إفشاءه، سواء في سبيل تحقيق المصلحة العامة، والأمن الاجتماعي؛ كحالات الإبلاغ عن الأمراض المعدية، والأوبئة، والجرائم، أو في سبيل مصلحة المريض الشخصية، كأن يرفض المريض علاجا ضروريا، لعدوى يحملها.

أما الإطار الآخر للحماية، فهو قانون حماية البيانات الشخصية، حيث اعتبرت البيانات الصحية، أو الطبية، فئة خاصة. فالبيانات الصحية، فئة من البيانات الحساسة، كما يوضح تعريف هذه الأخيرة، في القوانين الدولية، والعربية. وهي بالتالي، من البيانات الشخصية، التي يتشدد المشترع في حمايتها، ويحظر جمعها، ومعالجتها، إلا إذا توافرت الشروط القانونية، المنصوص عليها قانونا.

ففي عالمنا اليوم، تتوسع استخدامات تقنيات المعلومات والاتصالات، في المجال الطبي، وذلك، على جميع المستويات، بدءا من إدارة العيادات والمستشفيات، وملفات المرضى، مرورا بالاختراعات، وصولا إلى العلاج وتتبع المريض. وتسمح إنترنت الأشياء، في المجال الطبي، باتصال مباشر، ومتواصل، بكل ما يسجله جسد المريض، من تحولات، وردود فعل، وحركة طبيعية، من خلال أجهزة تزرع في جسده، أو تلصق عليه مباشرة.

كذلك، تعتمد التطورات العلاجية، في المجال الطبي الحديث، بشكل أساسي، على البيانات، التي تتجمع نتيجة إجراء الدراسات السريرية، والتي تهدف إلى إثبات

فاعلية وسلامة الأدوية، أو الأجهزة الطبية. ويتم إجراء هذه الدراسات، على عدد قليل من المرضى، فيما يستفيد من نتائجها، السكان المعنيون، على نطاق عالمي. لكن من النادر، أن نرى دراسات وأبحاث، تنفذ على آلاف من المرضى، نظراً للتكلفة العالية، من جهة أولى، وللصعوبات التنظيمية، التي ينطوي عليها التنفيذ، من جهة ثانية. وهذا يعني، إمكانية تسويق منتجات غير فاعلة عالميا، أو خطرة.

أما البيانات المعالجة، والمستخدمة في هذه الدراسات، فنادرا ما تم استخدامها، لاستخراج بيانات جديدة منها، إذ إنها تستخدم في الغالب، للتحقق من فرضيات الكفاءة، والسلامة، ولتقييم فعاليتها.

لكن دخول التقنيات الحديثة، إلى المجال الطبي، وأساليب معالجة البيانات، أفرزت وفرا من البيانات، ودفقا من المعلومات، شكلا مرتكزا جديدا للتقدم العلمي، في المجال الطبي، لاسيما من خلال ظهور مصادر جديدة للبيانات، ناتجة عن تجميع، وتقاطع قواعد بيانات، وتقنيات التحليل، والتنقيب. واصبح الطبيب، مركز هذه البيانات، والتقنيات، التي تساعده في التشخيص، وتحديد العلاج، ومتابعة المريض، وتطوير ممارساته المهنية.

فقد فتحت البيانات الضخمة، وعلم البيانات، وإنترنت الأشياء، فرصة للعلم في المجال الطبي، عبر ما تؤمنه من معلومات. إلا أن الإفادة من هذه الفرصة، يواجهها عدد من التحديات، الناجمة عن الأطر التنظيمية والتشريعية، الخاصة بحماية البيانات الشخصية، والتي يمكنها أن تعيق العديد من الاكتشافات، نتيجة منع الاستكشاف المنهجي للبيانات.

وتفترض معالجة البيانات الطبية في جميع الدراسات السريرية، موافقة واعية من المريض، يحدد فيه الاستخدام الذي سيتم إجراءه على البيانات، لاسيما لجهة التحليلات، ما يمنع إجراء أي استخدام لاحق لها؛ كتحليل البيانات الناتجة عن

تلك المعالجة، بسبب عدم التخطيط المسبق لذلك. علما، أن القوانين في الولايات المتحدة الأميركية، تميل إلى توسيع نطاق التحليلات، التي يمكن إجراؤها، في المرحلة النهائية، من مرحلة تصميم الدراسات السريرية.

وتقر بعض القوانين، موجبا على مضيف خدمات حفظ البيانات، بتأمين سلامتها، وأمنها، بحيث يأخذ جميع الإجراءات، والتدابير، التي تمنع انكشافها، أو الوصول إليها، بطريقة غير شرعية. ويمنع عليه نقلها، إلا عبر نظام من الشبكات، شديد الأمان. وغالبا، ما تجرم إتاحتها للآخرين، غير أصحاب الحق في الاطلاع عليها، كالموظفين العاملين على السجلات الطبية، أو الأطباء المعالجين، المعنيين بحالة المريض، أو أية جهة أخرى، تملك هذا الحق بموجب القانون؛ كوزارة الصحة، في بعض الحالات[108].

ويبقى أن الشرط الأساس، لاكتساب معالجة البيانات الطبية صفة المشروعية، هو موافقة الشخص المعني؛ أي المريض، بطريقة واضحة، صريحة، لا تحتمل التأويل.

وفي غياب تعريف قانوني، كان الفقه والاجتهاد، في الاتحاد الأوروبي، يحددان مدلول البيانات الشخصية، وما تشمله من معلومات، لكن القواعد الأوروبية الجديدة، حول "حماية الأشخاص الطبيعيين من المعالجة الإلكترونية والتدفق الحر للبيانات"، التي ألغت الإرشادات الأوروبية، أعطت تعريفا قانونيا، فاعتمدت ولأول مرة، تعريفا موحدا للبيانات الطبية، ارفق بعدد من الموجبات الخاصة بحمايتها[109]، وبحماية البيانات الشخصية، بشكل عام.

---

[108] - Healthcare Security: Understanding HIPAA Compliance and its Role in Patient Data Protection https://digitalguardian.com/blog/healthcare-security-understanding-hipaa-compliance-and-its-role-patient-data-protection

[109] - le règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - Article 4 - 15 «données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne; http://www.een-france.fr/document/129704-fiche-technique-le-reglement-europeen-relatif-a-la-protection-des-personnes-physique

وقد اعتبرت القواعد الجديدة، البيانات الطبية، كل معلومة، يمكنها أن تكشف الحالة الصحية، الجسدية، أو العقلية، لشخص طبيعي، بما في ذلك خدمات الرعاية، التي يحصل عليها. ويشمل هذا التعريف، أية معلومة، تتعلق على سبيل المثال، بالمرض، أو الإعاقة، أو العجز، أو الاستعداد المرضي، أو الملف الطبي، أو تحاليل مخبرية، أو علاج، وذلك بغض النظر عن مصدر المعلومة، سواء أكان الطبيب نفسه، أم المركز الطبي، أم المركز الاجتماعي، أم المستشفى.

كما حددت القواعد الأوروبية، البيانات الجينية[110]، المتعلقة بالخصائص الوراثية، الموروثة، أو المكتسبة، من شخص طبيعي، والتي تنقل معلومات فريدة حول علم وظائف الأعضاء، أو الحالة الصحية. كما حددت البيانات البيومترية[111]، الناتجة عن معالجة تقنية محددة، حول الخصائص الفيزيولوجية لشخص طبيعي، أو سلوكياته.

وقد احتفظت هذه القواعد، بمبدأ حظر معالجة هذه البيانات، كما فعلت الإرشادات الأوروبية، وأرفقته بعدد من الاستثناءات، التي تختص أيضا، بالبيانات الحساسة الأخرى، كـ: الموافقة الواعية من الشخص المعني، والمصلحة العامة، والبحث العلمي، والطب الوقائي، على سبيل المثال.

وفيما اكتفى كل من المشترع المصري، والمغربي، والموريتاني، والتونسي، بذكر البيانات الصحية، من ضمن تعريف البيانات الحساسة، وتخصيصها بأحكامها، خصص القانون التونسي، القسم الثاني، من الباب الخامس منه، لمعالجة هذه

[110] - le règlement européen relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données
Article 4 - Définitions.«données génétiques», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

[111] - Le règlement européen relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données - Article 4 - Définitions.«données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

البيانات، في المواد 62 إلى 65. وقد تناولت المواد المذكورة، تفاصيل شروط المعالجة، التي تعتبر محظورة أساسا. فركزت على صفة الأشخاص، الذين يمكن أن ينفذوا هذه العملية، فحصرتها بالأطباء، أو بأشخاص خاضعين بحكم مهامهم، إلى واجب المحافظة على السر المهني.

وإذ أقرت إمكانية إحالة هذه البيانات، من الطبيب إلى باحثين، أو مؤسسات البحث العلمي الصحي، إلا أنها اشترطت لذلك، تقديم طلب من الجهة التي تريد الحصول على البيانات، والحصول على ترخيص من الهيئة الوطنية لحماية المعطيات الشخصية. وقد أعطيت الهيئة، حق تحديد الاحتياطات والإجراءات، الواجب اتخاذها، لضمان حماية البيانات الشخصية المتعلقة بالصحة، إضافة إلى حق منع نشرها.

» شمولية المبدأ

يغطي مفهوم معالجة البيانات، في القواعد الأوروبية الجديدة، مروحة واسعة من العمليات المادية أو الإلكترونية، التي تطاول البيانات الشخصية، بما فيها، جمع البيانات، أو تسجيلها، أو تنظيمها، أو تخزينها، أو تحويرها، أو استرجاعها، أو مراجعتها، أو استعمالها، أو الكشف عنها بنقلها، أو إذاعتها، أو توزيعها، أو إتاحتها، أو التقييد، أو المسح، أو التدمير.

كما يشمل هذا المفهوم، المعالجة اليدوية البحتة، إذا كانت جزءا من نظام حفظ بيانات منظم. وتدخل في هذا المفهوم، العمليات التي تطاول إدارة شؤون الموظفين، وإدارة المرتبات، والوصول إلى، أو مراجعة قاعدة بيانات الاتصالات، التي تحتوي بيانات شخصية، وإرسال رسائل البريد الإلكتروني الترويجية، وإتلاف الوثائق التي تحوي بيانات شخصية، ونشر صور أو بيانات الأشخاص على الإنترنت، وتخزين عناوين الأجهزة الإلكترونية IP، أو تسجيل الفيديو والأفلام التصويرية.

- معالجة البيانات

ترتكز هذه العملية في جوهرها على التعامل مع البيانات الشخصية، وتحتل على هذا الأساس، حيزا واسعا في القوانين، وتتطلب التطرق إلى مسائل عدة متفرعة، نستعرضها كما يأتي.

ورد تعريف عمليات المعالجة، في جميع القوانين العربية الصادرة في هذا المجال، انطلاقا من نوعية العمليات التي تطال البيانات، مع المساواة بين اليدوي منها والآلي. وذلك، بدءا من عملية جمعها، مرورا باستلامها، وحفظها، وتنظيمها، وتخزينها، واسترجاعها، وطرق استخدامها، وتحليلها، وصولا إلى استثمارها، وتوزيعها، ونشرها، ومحوها أو إتلافها. وقد حرصت بعض النصوص، على عدم التمييز بين الوسائل، التي تنشر بواسطتها هذه المعلومات، كالإرسال، أو الإذاعة، أو الإنترنت.

وقد تميز القانون التونسي، بإضافة ذكر قواعد البيانات، والفهارس، والسجلات، أو البطاقات[112]. علما انه يمكننا اعتبار هذه الإضافة، محاولة توضيح وتركيز للمفهوم، على غرار ما كان قد اعتمد في القواعد الإرشادية الأوروبية، الصادرة في العام 1995، والقواعد الأوروبية الجديدة، الصادرة عام 2016، والتي دخلت حيز التنفيذ، في أيار 2018، نظرا لشمولها في تعريف المعلومات الشخصية، بعبارات، مثل: "بغض النظر عن دعامتها، ومصدرها".

وورد أيضا، ذكر صريح في مجمل القوانين، لخضوع معالجة البيانات الشخصية، في القطاعين العام والخاص، للقواعد التي تحكم حماية البيانات الشخصية، دون تمييز. كما خصصت مواد لتفصيل حماية البيانات الصحية، التي تتم في إطار دراسة، وتقييم

---

[112] - الفصل 6 يقصد في مفهوم هذا القانون ب :
معالجة المعطيات الشخصية : العمليات المنجزة سواء بطريقة آلية أو يدوية من شخص طبيعي أو معنوي والتي تهدف خاصة إلى جمع معطيات شخصية أو تسجيلها أو حفظها أو تنظيمها أو تغييرها أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو إتلافها أو الاطلاع عليها وكذلك جميع العمليات المتعلقة باستغلال قواعد البيانات أو الفهارس أو السجلات أو البطاقات أو بالربط البيني،
البطاقة: مجموعة من المعطيات الشخصية المنظمة والمجمعة والتي يمكن النفاذ إليها وفق معايير محددة وتمكن من التعرّف على شخص معيّن،

المعطيات المرتبطة بالعلاج، أو بالوقاية، سواء تعلق الأمر بالمتابعة العلاجية، أو الطبية الفردية للمرضى، والتي يقوم بها الأفراد في مراكز العلاج، أو الأطباء، أو شركات التأمين، أو الباحثون في المجال الطبي، والوقاية الصحية، وغيرهم.

» الاستثناءات

إذا كان المبدأ العام، هو السماح بمعالجة البيانات الشخصية، شرط مراعاة الأحكام، والقوانين التي ترعى قواعد ومبادئ حمايتها، إلا أن لهذا المبدأ استثناء، يقضي بمنع معالجة بعض البيانات. ويبنى الاستثناء، من جهة أولى، على طبيعة ومستوى المخاطر، التي يمكن أن يشكلها المحتوى؛ كما هو الحال مع البيانات الحساسة، والبيانات الوراثية، أو الجرائم، والأحكام الجزائية، ورقم التسجيل الموحد في الدليل الوطني للأشخاص الطبيعيين، والأوضاع الاجتماعية الصعبة للأشخاص، والبيانات البيومترية، بينما يبنى، من جهة ثانية، على الهدف من المعالجة، وإنشاء الملفات، كما هو الحال، مع المعالجة بهدف استبعاد بعض الأشخاص، من الإفادة من بعض الحقوق، أو الخدمات، أو العقود، أو كما هو حال الملفات التي تتقاطع مع ملفات أخرى، لأهداف تختلف عن أهداف المعالجة الأساسية.

ونشير في هذا السياق، إلى الأنظمة البيومترية، التي تتعرف على الشخص، من خلال خصائصه الطبيعية، والمورفولوجية، والجينية، والتي تسمح لأرباب العمل، أو حتى لبعض الإدارات الرسمية، باستبعاد الأشخاص الذين يعتبرون حاملي الكثير من المخاطر الطبية، من خلال التعرف على البيانات الواردة في الجينوم.

كما يمكن لهذه الأنظمة، المساهمة في مجال الطب الوقائي، وتحديد الأشخاص الأكثر عرضة لحوادث العمل، نتيجة تحليل وراثي لهم، بحيث يخصون بمتابعة، ورعاية طبية خاصة. يضاف إلى ذلك، إمكانية لجوء شركات التأمين، إلى استخدام أنظمة مماثلة، تمكنها من إدارة عملية اختيارها لزبائنها، وتحديد أقساط التأمين، بطريقة

فضلى تخدم مصالحها، لناحية مساعدتها على الحد من احتمالات اضطرارها إلى تحمل أعباء الطبابة. وفي كل ما تقدم، إمكانية كبرى، للجنوح نحو التمييز بين الأشخاص.

ويمكن الإشارة هنا أيضا، إلى قدرات التكنولوجيا على استخراج تصنيفات، وتشخيصات، وتوقعات، بخصوص الحالة الصحية للأشخاص، والتي بدت واضحة، في دراسة أجرتها مايكروسوفت، حول كيفية اكتشاف مرضى السرطان، من بين مستخدمي محركات البحث، عبر تحليل بياناتهم الشخصية[113]. علما أن الإرشادات الأوروبية، كانت قد سمحت، بمعالجة هذه البيانات، لأهداف الطب الوقائي[114]

وجرت العادة أن تخضع بعض القوانين، إنشاء الملفات الخاصة بأمن الدولة، أو الدفاع، أو العقوبات الجزائية، كما ملفات رقم التسجيل الموحد في الدليل الوطني للأشخاص الطبيعيين، إلى تدابير خاصة قبل إنشائها، كالحصول على إذن بالمعالجة، بمقتضى مرسوم، بعد استشارة السلطة الوطنية لحماية البيانات الشخصية.

وكانت الإرشادات الأوروبية لعام 1995، قد نصت في المادة الثالثة منها[115]، على استبعاد الملفات والبيانات، التي تنشأ لأغراض الأمن العام، والدفاع، وأمن الدولة، بما فيها الأمن الاقتصادي، أو الملفات، التي يكون لمعالجتها ارتباط بنشاطات الدولة في المجال الجزائي.

---

[113] - Microsoft Finds Cancer Clues in Search Queries
https://www.nytimes.com/2016/06/08/technology/online-searches-can-identify-cancer-victims-study-finds.html

[114] - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Article 7. - 3. Le paragraphe 1 ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

[115] -Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Article 3 - Champ d'application
2. La présente directive ne s'applique pas au traitement de données à caractère personnel:
- aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

في هذا السياق، استبعدت المادة الثامنة من الإرشادات[116]، تطبيق أحكامها على فئات معينة من البيانات، وهي ما يعرف بالبيانات الحساسة، والتي يأتي ضمنها البيانات التي تكشف الأصول العرقية، أو الإثنية، والآراء السياسية، والمعتقدات الدينية والفلسفية، والانتماء النقابي، إضافة إلى بيانات الصحية، والحياة الجنسية، كما أسلفنا.

في المقابل، تجمع القوانين العربية، وعلى غرار جميع القوانين المعمول بها حول العالم، على عدد من الاستثناءات، التي لا بد منها، لضمان التوازن المطلوب، بين حق الفرد في حماية حقوقه وحرياته الأساسية، وحق المجتمع في التمتع بالرفاه، والأمن، والاستقرار، من جهة أولى، ولممارسة الدولة لواجباتها، في هذه المجالات، من جهة ثانية.

من جهته، أخضع القانون الموريتاني، معالجة البيانات التي تتعلق بالأمن "العمومي"، والدفاع، والبحث، ومتابعة الجرائم الجزائية، أو أمن الدولة، لقانون "حماية البيانات ذات الطابع الشخصي"[117]، بغض النظر عن ارتباطها بمصلحة الدولة، مع مراعاة الاستثناءات الواردة في قانون الحماية، أو أية قوانين أخرى. وكان هذا القانون، قد حظر، في المادة 12 منه، معالجة البيانات الحساسة، معددا الحالات الاستثنائية، التي تجيز معالجتها، ومن بينها، حالات تتعلق بمصلحة الدولة، بطريقة مباشرة، أو غير مباشرة، كتحقيق العدالة، والتحقيقات الجنائية، أو تنفيذ مصلحة عامة.

ومن الطبيعي، أن تتقدم الاستثناءات، معالجة البيانات، في إطار الاستعمال الشخصي، أو العائلي، ولأهداف شخصية، من قبل شخص طبيعي، شرط عدم نشرها، أو توزيعها، أو استثمارها، أو نقلها إلى الغير. أما السبب الذي يقدم في

[116] - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - Article 8 - Traitements portant sur des catégories particulières de données
1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

[117] - المادة الثالثة، من القسم الثالث، فقرة 5.

تبرير هذا الأمر، فهو غياب مخاطر انكشاف البيانات الشخصية، على نحو يهدد الحياة الخاصة، أو الحقوق الأخرى. وقد اقر هذا الاستثناء منفردا، في المادة الثالثة من التشريع التونسي[118]، بينما دمجت الاستثناءات الأخرى، في مواد تتعلق بمسؤولية وموجبات المعالج.

كذلك، خرجت فئات المعلومات الشخصية، التي تجمعها الدولة وتعالجها، في إطار نشاطها المعتاد، كسلطة عامة، مسؤولة عن ضمان الأمن والسلم الوطنيين، عن نطاق هذه القوانين. وترد في هذا الإطار، استثناءات البيانات المتعلقة بالجنايات، والتي غالبا ما تكون محفوظة ضمن قواعد بيانات قضائية، أو أمنية، بإدارة السلطات العامة المسؤولة عن مكافحة الجريمة، ومعاقبتها، ورصدها، والوقاية منها. وكذلك، استثني ما يجمع من بيانات ومعلومات، في إطار الحفاظ على الأمن القومي، وضرورات الدفاع الوطني.

وقد لحظ التشريع القطري، تفصيلا لبعض الحالات، التي يمكن اعتبارها من مكونات الأمن القومي، كاستقرار وحماية علاقات الدولة، ومصالحها الوطنية، مع الدول الأخرى، وحماية الاقتصاد، ومالية الدولة. كما نصت المادة الثامنة عشرة، على ضرورة تخصيص سجل خاص، تقيد به البيانات المجموعة والمعالجة في هذا الإطار، على أن تحدد شروط، وضوابط، وأحوال القيد فيه، بقرار من الوزير المختص. إضافة إلى ذلك، استثنيت المعالجات، لغرض الإحصاءات الرسمية.

وكذلك فعل التشريع المصري، باستثنائه معالجة المعلومات التي تتعلق بقضايا الإرهاب، وإشكال الجريمة المنظمة كافة، مع إقرار موجب عودة الجهاز الذي يجمع ويعالج البيانات الشخصية، في هذا الإطار، إلى جهاز حماية البيانات الشخصية، لإعلامه بطبيعة البيانات التي بحوزته، والغرض من معالجتها، وتبيان أهميتها لدعم التحقيق.

[118] - الفصل 3 لا ينطبق هذا القانون على معالجة المعطيات الشخصية لغايات لا تتجاوز الاستعمال الشخص ي أو العائلي بشرط عدم إحالتها إلى الغير

وفي هذه القاعدة، إصرار واضح، على تأمين إطار حماية فاعل، وإيجاد توازن بين المصالح العامة والخاصة، بما يمنع الاعتداء على الحقوق والحريات، خارج إطار الرقابة. كما استثنيت كذلك، وعلى غرار بقية القوانين، عمليات المعالجة لأهداف إحصائية رسمية، أو لتطبيق نص تشريعي مستقل. وغني عن القول، إن الحالة الأخيرة من الاستثناءات، هي معالجة البيانات التي يمكن أن تتصل، بإجراءات وأصول سير العدالة، المنصوص عنها في قوانين خاصة، أو ما يتصل بقواعد القانون المدني أو الجزائي، أو غيرهما من القوانين العامة والخاصة.

أما القانون المغربي، فقد نص في المادة الثانية منه، التي تتناول نطاق التطبيق، على شرط خاص بالبيانات، التي تجمع تطبيقا لنص تشريعي،حيث فرض إرسال مشاريع أو مقترحات القوانين، الخاصة باستحداث ملفات متعلقة بالبيانات المذكورة، إلى اللجنة الوطنية لحماية البيانات، مع تعيين الجهة المسؤولة عن الملف، والغاية المتوخاة منه، وتحديد فئات الأشخاص المعنيين بالبيانات، ومصدر هذه الأخيرة، والجهات الثالثة التي يمكن أن تنتقل إليها، مع بيان الإجراءات المتخذة لضمان سلامتها، وعدم انكشافها.

« شروط المعالجة

تتعدد هذه الشروط، وتتكامل بطريقة تؤشر، إلى أهمية هذه المسألة، التي تتوزع على أساسها المسؤوليات، والموجبات، والحقوق. وسنبدأ في عرضها من التصريح، الذي لم يعد واردا، وفقا للقواعد الأوروبية الجديدة، واستعيض عنه، بتشديد موجب الحماية، والالتزام بأحكام القانون.

وتعتبر الشروط التي أقرت للسماح بمعالجة البيانات الشخصية، في القوانين العربية، سواء من حيث الأصول الإدارية المفروضة، أم من حيث ضرورة احترامها حقوق صاحب البيانات، منسجمة مع النصوص الدولية والأوروبية. ويبدو واضحا تأثر

القوانين بالتوصيات الأوروبية لعام 1995، وانسجامها مع الأهداف المرجوة من إقرارها، لاسيما منها، الحماية عبر إطار تشريعي، يضمن وضوح الخطوات العملية، التي تحصل في هذا المجال.

» التصريح أو إعطاء العلم

إذا تركنا جانبا، تميز التشريع الأوروبي الجديد، الذي دخل حيز التنفيذ، في 25 أيار/مايو الحالي، عن التوصية الأوروبية لعام 1995، وعن القوانين الفرنسية، لناحية إلغائه مرحلة التصريح المسبق، تبقى شروط المعالجة، بحسب القوانين العربية الحالية، منسجمة مع مستوى الحماية المطلوب. فقد أخضعت المعالجة، بشكل عام، إلى تصريح مسبق، بينما نص القانون، على ضرورة الحصول على ترخيص، في حالة البيانات الحساسة.

وقد لحظ القانونان المغربي والتونسي[119]، ضرورة التصريح المسبق، من قبل المسؤول عن المعالجة، لدى السلطة الوطنية المختصة بحماية البيانات الشخصية، على أن يحصل على وثيقة تثبت حصول التصريح. ويعتبر عدم اعتراض الهيئة، خلال مهلة محددة، بمثابة الموافقة

كذلك، فرض كل من المشترع المصري، والمغربي، والتونسي، في حالة البيانات ذات الطابع الخاص، العودة إلى الجهة المختصة بحماية البيانات، مع تعيين كل العناصر التي تسمح لهذه الأخيرة، بإجراء رقابة على مدى الالتزام بمعالجة، لا تتعرض لحقوق الشخص المعني، ولا تسيء إليه. ويعتبر هذا الأمر، بمثابة تفعيل للحماية، في مواجهة مخاطر استعمال المشرع لعبارات، يعتبرها البعض فضفاضة، مثل "الأمن القومي".

[119] - الفصل 7 تخضع كل عملية معالجة معطيات شخصية لتصريح مسبق يودع بمقر الهيئة الوطنية لحماية المعطيات الشخصية مقابل وصل أو بواسطة رسالة مضمونة الوصول مع الإعلام بالبلوغ أو بأي وسيلة أخرى تترك أثرا كتابيا . ويقدم التصريح من قبل المسؤول عن المعالجة أو ممثله القانوني . ولا يعفي التصريح من المسؤولية إزاء الغير . وتضبط شروط تقديم التصريح وإجراءاته بأمر . ويعتبر عدم اعتراض الهيئة على معالجة المعطيات الشخصية في أجل شهر بداية من تاريخ تقديم التصريح قبولا

بشكل عام، يفرض القانون إتمام إجراءات مسبقة، قبل البدء بأية عملية لمعالجة بيانات شخصية، وذلك تحت طائلة إنزال عقوبات جزائية، بحق من لا يتقيد بها. وتتنوع هذه الإجراءات، بين التصريح، أو الإعلام البسيط، أو تقديم طلب، للحصول على ترخيص بالمعالجة. ويعتبر هذا الأمر، من أساسيات مبدأ الشفافية، كونه يفتح أمام السلطة المختصة، ليس فقط إمكانية ممارسة مهمتها، في اطلاع المعنيين على وجود ملفات لمعالجة البيانات، والفئات التي تعالج منها، بل يتيح أيضا، إجراء الرقابة اللازمة، على مدى تقيد مسؤول المعالجة، بالأحكام القانونية المقررة، والتوصيات، والإجراءات.

ويعتبر عدم إتمام هذه الأخيرة، مانعا لإقرار مشروعية أي قرار يتخذ، بناء على البيانات الشخصية التي تم جمعها. وكانت محكمة التمييز الفرنسية، الغرفة الاجتماعية، قد اعتبرت قرار الصرف من الخدمة، غير قانوني، كونه استند إلى عدم تأشير الموظف على جهاز تسجيل الحضور، باستخدام بطاقة الوظيفة، لان الجهاز كان يعمل على جمع بيانات الموظفين الشخصية، دون إتمام موجب التصريح إلى هيئة حماية البيانات[120].

في المقابل، تعتمد إجراءات بسيطة ومبسطة، لكل عملية ضرورية لتنفيذ العمل، لا تثير تحديات كبيرة، أمام حماية الحقوق والحريات؛ كحالة أصحاب المواقع التجارية الإلكترونية، الذين يجمعون ويعالجون، بيانات زبائنهم، لإدارة تسليم الطلبات، ودفع الأتعاب، وإعطاء ميزات وحسومات خاصة. وفي هذه الحالة، يمكن أن يكون التصريح مجرد إبلاغ، عن الالتزام بمعيار معين، أو إجراءات مطلوبة قانونا.

[120] - M. X salarié de la société depuis 1993, a été licencié le 30 avril 1998 en raison de son refus à 19 reprises entre février et avril 1998 d'utiliser son badge à la sortie de l'entreprise ; que l'arrêt attaqué (Nancy, 25 juin 2001) a dit que le licenciement était sans cause réelle et sérieuse en raison du défaut de déclaration du traitement à la Commission nationale de l'informatique et des libertés ; cass. Soc. 6 Avril 2004 https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007048556

» الحصول على إذن أو تصريح

أما فيما يتعلق بالبيانات الحساسة، فانه لا يكتفي بالتصريح، بل غالبا، ما تفرض إجراءات اكثر تعقيدا، كأن يفترض الحصول على إذن خاص، من السلطة المعنية بحماية البيانات. ويفرض هذا الإجراء الإداري الخاص، بناء لطبيعة البيانات (جينية، أحكام جزائية، ...)، أو بسبب كون الأهداف محددة وخاصة (حرمان بعض الأشخاص من حق ما)، وأما بسبب النية في نقل البيانات، إلى خارج الحدود الوطنية. ويمكن أن يصدر هذا الإذن عن الهيئة، أو بموجب قرارات وزارية، أو بمرسوم عن هيئة قضائية كمجلس شورى الدولة، ولكن دائما، بعد إعطاء الهيئة المختصة رأيها.

وتقر بعض القوانين، إجراءات إدارية مختلفة، باختلاف طبيعة الجهة مقدمة طلب الحصول على إذن، كان تكون من القطاع العام، أو القطاع الخاص. إلا إنها تتلاقى، على ضرورة تشديد شروط المعالجة، وإعلام أصحاب البيانات، نسبة إلى المخاطر التي تمثلها، على مستوى الحقوق والحريات.

كذلك، يذهب بعضها إلى إقرار عقوبات جزائية، على عدم التقيد بالإجراءات الإدارية، دون التمييز، بين عدم التقيد المقصود، أو غير المقصود. كأن يكون المسؤول عن المعالجة قد نسي التصريح، أو أن يكون قد قصد عدم القيام به. وكان الاجتهاد الفرنسي، قد اتخذ عددا من القرارات في هذا الاتجاه، معتبرا أن مجرد عدم إتمام الإجراءات المفروضة، سبب كاف للإدانة[121].

وقد اعتبرت المحكمة، في هذه القضية، إن مجرد تسجيل معلومات حساسة عن موظفي الشركة، ولو في ملف ورقي غير معد للمعالجة الإلكترونية، يهدف إلى تقييم الموظفين، دون الاستحصال على إذن بذلك، من هيئة حماية البيانات الشخصية،

[121] - Les fichiers du personnel sous contrôle de la Cnil
https://www.01net.com/actualites/les-fichiers-du-personnel-sous-controle-de-la-cnil-179815.html

يعتبر انتهاكا لقانون حماية البيانات، ويستوجب العقوبة المقررة لذلك.

» رقابة السلطات العامة على معالجة البيانات

مما لا شك فيه، إن القواعد الإرشادية الأوروبية، كما التوصيات الصادرة في العام 1995، تتجه بشكل أساسي، لإخضاع الجهات الاقتصادية، العاملة ضمن الاتحاد الأوروبي، كما غيرها من أشخاص القانون العام والخاص، إلى المبادئ الأساسية لحماية البيانات.

لكن هذه النصوص، لا تطبق على المعالجات التي تقوم بها أجهزة الدولة الأمنية، كالأمن الداخلي، والدفاع، والأمن العام، والإدانات والعقوبات الجزائية. وكانت محكمة العدل الأوروبية، قد أصدرت قرارا، بهذا المعنى، مستبعدة معالجة البيانات الشخصية، التي تقوم بها الدولة، في مجال تنظيم الإقامة[122]، من نطاق هذا الاستثناء.

كما نظرت المحكمة، في قضية تقدم بها احد المواطنين النمساويين، لمحو بياناته، من سجل يحوي بيانات شخصية، إضافة إلى معلومات عن تاريخ الدخول إلى ألمانيا، والخروج منها، كما يحوي أحياناً، معلومات عن قرارات الإبعاد عن الأراضي الألمانية، في حال ارتكاب جرائم خطرة، كالأعمال الإرهابية، أو الاتجار بالمخدرات، أو مخالفة قوانين الهجرة.

فرأت أن هذه البيانات، تستخدم في إطار تنظيم إقامة الأجانب، كما تستخدم لغايات إحصائية، ولمكافحة الجريمة، في الوقت الذي لا توجد فيه ملفات مشابهة، خاصة بالمواطنين الألمان.

[122] - ec.europa.eu/dgs/legal_service/arrets/06c524_fr.pdf
c-524/06 Huber contre république fédérale d'Allemagne, arrêt du 16 décembre 2008

وعليه، فقد ذهبت في قرارها، إلى اعتبار معالجة البيانات، بمثابة تمييز على أساس الجنسية، من حيث هدفها، الذي هو مكافحة الجريمة، الأمر الذي تحظره القوانين الأوروبية الوطنية، كما تحظره الإرشادات الأوروبية، والتي اعتبرت إن مشروعية المعالجة، تنتج عن ضرورة المعالجة، لتنفيذ مهمة ذات منفعة عامة، أو مرتبطة بممارسة السلطات العامة.

وفي قرار آخر[123]، تناولت المحكمة، مسألة معالجة إحدى السلطات المحلية، لبيانات شخصية، فأكدت مرة أخرى، خضوع أشخاص القانون العام للقواعد الإرشادية، إلا متى كان هذا النشاط، مستبعدا صراحة، في القواعد، وبالتالي، ما يؤخذ بعين الاعتبار هنا، هو هدف المعالجة، لا صفة الجهة التي تقوم بها، لتقرير خضوعها، للقواعد الإرشادية الخاصة بحماية البيانات الشخصية.

في هذا الإطار، خصص المشرع التونسي، الباب الخامس منه، لأصناف خاصة من المعالجة، أورد فيها تحت القسم الأول: "معالجة المعطيات الشخصية من الأشخاص العموميين"، والمقصود بهم أجهزة الدولة.

أما بقية القوانين العربية، فقد أخضعت الدولة، وإداراتها، لمبادئ حماية البيانات الشخصية، من خلال نطاق التطبيق، كما فعل المشترعان المصري، والمغربي، عندما فرضا موجب إعلام الهيئة الوطنية لحماية البيانات، حتى في حالات التحقيقات القضائية، والإرهاب، والجريمة المنظمة.

- نقل البيانات خارج الحدود

يشكل انتقال البيانات، أو تبادلها، الحركة الأهم، التي تتسم بها البيانات في الفضاء السيبراني، وعلى الإنترنت، حين تنتقل بين الشبكات، والتطبيقات، وقواعد المعلومات، والمخدمات، وغير ذلك، من الأجهزة والبرامج، التي تعالجها لتتم عملية

[123] - CJUE 7 Novembre 2013 "X. contre Bois-le-Duce" Aff. C-473/12

نقلها، أو حفظها، أو توزيعها، أو أية عملية أخرى من أنواع المعالجة، التي تساعد في الاطلاع عليها.

ويشكل انتقال البيانات خارج الحدود الوطنية، البعد العالمي، لعملية معالجة البيانات، وحق الحفاظ على الحياة الخاصة. ويعتبر هذا الانتقال، من الناحية القانونية، نسبة إلى مبدأ السيادة الإقليمية، إخراجا لها من نطاق تطبيق القوانين المحلية، وصلاحية السلطات الوطنية. لذلك، كان من البديهي، أن يعطى هذا البعد، اهتماما أساسيا، في قوانين حماية البيانات الأوروبية، بحيث تضمن عنوان إرشادات منظمة التعاون الاقتصادي والتنمية، كما الإرشادات الأوروبية الصادرة عام 1995، والقواعد الأوروبية الجديدة، مصطلح: "نقل البيانات خارج الحدود"، و"الحركة الحرة لهذه البيانات".

وكانت إرشادات 1995، قد حظرت، في المادة الأولى[124] منها، على الدول الأعضاء في الاتحاد، منع التدفق الحر للبيانات، أو الحد منه. وكذلك، فعلت القواعد الأوروبية الجديدة، التي دخلت حيز التطبيق، منذ أواخر أيار / مايو 2018، حين احتفظت بهذا البعد، في[125] الفصل الخامس، الذي حمل عنوان "نقل البيانات إلى دول ثالثة، أو منظمات دولية". وقد أبرزت مواد هذا الفصل، عددا من الشروط، التي تمحورت حول المبدأ العام الذي يحكم نقل البيانات، ويؤمن استمرار حماية الأشخاص وحقوقهم. فاعتبرت أن عملية النقل، لا تحتاج إلى إذن خاص، عندما تتوافر الأطر القانونية المناسبة للحماية، في البلد المعني بتلقي البيانات.

---

[124] - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Art.1 Objet de la directive - Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel
Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.

[125] - CHAPITRE V - Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales
https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article49

وينطبق هذا الأمر، على القطاعات والشركات، والمنظمات التابعة للاتحاد الأوروبي، أو العاملة على ارضه، والخاضعة لقوانينه. علما أن تقييم الإطار التشريعي المناسب، يتم من قبل سلطة الحماية الأوروبية، بناء على مؤشرات تتعلق بالنظام القانوني المعتمد، في البلد المذكور، ومدى احترامه لحقوق الإنسان، سواء أكان ذلك، في القوانين العامة، أم الخاصة بقطاعات معينة، بما فيها أنظمة الدفاع، والأمن العام، والقوانين الجزائية، وحق السلطات العامة في الوصول إلى البيانات الشخصية، وشروط إعادة نقل البيانات إلى بلد ثالث آخر، أو منظمة دولية، والحقوق التي يمكن الاعتداد بها، من قبل الأشخاص المعنيين بالبيانات المنقولة، والمراجعات القضائية والإدارية، التي يمكن أن يلجأ إليها هؤلاء.

ومن المؤشرات على وجود أطر قانونية مناسبة للحماية، وجود سلطة مستقلة أو اكثر، معنية بحماية البيانات الشخصية، تتعاون مع الاتحاد، ولها القدرة على ممارسة صلاحيات فاعلة، في هذا المجال، تضمن تطبيق قوانين الحماية، ومساعدة الأشخاص المعنيين، وتوجيههم، في كيفية ممارسة حقوقهم. على خط متصل، تؤخذ بعين الاعتبار، التزامات الدول الثالثة، أو المنظمات الدولية، بمقتضى اتفاقيات، أو عقود، أو أية وسيلة قانونية ملزمة، دولية، أو إقليمية، لاسيما ما يتعلق منها، بحماية البيانات ذات الطابع الشخصي.

» **درع الحماية**[126]

في سياق متصل، وعلى المستوى الدولي، وقع الاتحاد الأوروبي مع وزارة التجارة الأميركية، في 12 تموز/ يوليو، على إطار عمل خاص بحماية الخصوصية، أطلق عليه اسم "درع الخصوصية"[127]، بعد ما تبين قصور اتفاق المرفأ الآمن، الموقع سابقا بينهما، عن تأمين الحماية اللازمة للبيانات العابرة للأطلسي، وذلك، في إطار

[126] - https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en
[127] - Privacy Shield

السعي لدعم التجارة عبر الأطلسي، وحماية الحقوق الأساسية للأفراد، في الاتحاد الأوروبي

ويقضي هذا الإطار، بتزويد الشركات على جانبي الأطلسي، بآلية تساعد على الامتثال، لمتطلبات حماية البيانات المنصوص عليها في القواعد الأوروبية الجديدة، عند نقل البيانات الشخصية إليها، من جهة أولى، وعند استخدامها، من جهة ثانية. كما يضمن هذا الإطار، استمرار توافر المستوى المطلوب من الحماية، عندما يتم نقل البيانات، التي جمعت ضمن هذا الإطار، إلى جهات ثالثة.

وإضافة إلى إلزام المسؤولين عن المعالجة في الشركات العاملة في الولايات المتحدة الأميركية، بمبادئ معالجة البيانات الشخصية، وأسس الشفافية، والمحاسبة، التي ينص عليها التشريع الأوروبي، يتميز هذا الدرع، باحتوائه على مجموعة من وسائل الحماية الصارمة، والقابلة للتنفيذ، لاسيما وأنها توفر بيئة ملائمة لممارسة الحقوق الفردية؛ كالوصول إلى عدد من القنوات لمعالجة مخاوفهم، حول امتثال الجهات المشاركة في الإطار، بما في ذلك الوصول إلى العدالة، من خلال الحل المجاني للنزاعات، والإشراف الجدي من قبل الحكومة الأميركية، على آلات التنفيذ، في الولايات المتحدة الأميركية، وتعزيز التعاون مع سلطات الحماية في الاتحاد الأوروبي.

ولهذه الغاية، يفترض أن تحصل الشركات المقيمة في الولايات المتحدة الأميركية، والراغبة في الإفادة من هذا الإطار، على مصادقة وزارة التجارة الأميركية، والقيام من ثمّ، بإعلان التزامها بالامتثال لمتطلبات درع الحماية، في سياسة الخصوصية، التي تنشرها على موقعها، بما يجعل الالتزام قابلا للتنفيذ، بموجب القوانين الأميركية.

كما يفترض بأية جهة تمارس نشاطها على الإنترنت، أن تضيف وصلة إلى درع الخصوصية، الموجود على موقع لجنة التجارة الفدرالية، وأخرى إلى الجهة المعنية

بتلقي الشكاوى. وعلى خط متصل، يفترض بالشركات الراغبة في الانضمام إلى هذا الإطار، مراجعة آليات الحماية لديها، على جميع المستويات، التقنية، والفنية، والإدارية. وقد أقرت الاتفاقية عددا من الحقوق والالتزامات، ومنها:

- يجوز للأفراد تقديم شكوى مباشرة، إلى أي طرف من المشاركين في درع الخصوصية، ويجب على المشارك الرد، في غضون 45 يوماً.
- يجب على المشاركين في درع الخصوصية، أن يوفروا مجانا، آلية مراجعة مستقلة، يمكن من خلالها التحقيق في شكاوى ونزاعات كل فرد، وتسويتها على وجه السرعة.
- إذا قدم أحد الأفراد شكوى إلى هيئة حماية البيانات[128]، في الاتحاد الأوروبي، تلتزم وزارة التجارة الأميركية، بتلقيها، والمراجعة بخصوصها، وبذل أفضل الجهود، لتسهيل حلها، وتأمين الرد في مدة أقصاها 90 يوماً.
- تلتزم لجنة التجارة الفيدرالية الأمريكية[129]، بالعمل عن كثب، مع سلطات الحماية في الاتحاد الأوروبي، لتقديم المساعدة على تنفيذ امتثال الشركات الأميركية، بما في ذلك مشاركة المعلومات، والمساعدة في التحقيق، وفقًا لقانون الويب الآمن[130]، الذي يعطي اللجنة صلاحية التعاون، مع السلطات الأجنبية، المعنية بإنفاذ القوانين، من خلال توفير الإثباتات الضرورية لها، للقيام بتحقيقات مناسبة، وتنفيذ القوانين.
- تلتزم لجنة التجارة الفدرالية، بتنفيذ صارم لأحكام درع الخصوصية، من خلال إيلائها الأولوية للإحالات، التي تتم من قبل سلطات الحماية الأوروبية، ووزارة التجارة، وهيئات التنظيم الذاتي للخصوصية، أو من أية مراجعة مستقلة. وتتعهد اللجنة، في هذا المجال، بخلق مرجعية موحدة للإحالة، تعين فيها جهة

[128] - Data Protection Authorities (DPA)

[129] - Federal Trade Commission (FTC)

[130] - The U.S. SAFE WEB Act is a law that gives the Federal Trade Commission (FTC), a U.S. government agency, the authority to provide evidence to foreign law enforcement agencies to support appropriate foreign investigations or enforcement actions.

اتصال خاصة، بالإحالات التي تقدمها هيئات الحماية الأوروبية، وتأمين تبادل المعلومات، حول الإحالات مع سلطات تنفيذ القانون، مع مراعاة قوانين وقيود السرية.

» على المستوى العربي

وفي هذا الإطار، جاء نص القانون المغربي، في المادة 43، من الباب الخامس، على نقل المعطيات نحو بلد اجنبي، منسجما مع التوجه الأوروبي، عندما منع على المسؤول عن المعالجة، نقل هذه البيانات، ما لم تضمن الدولة المتلقية، مستوى حماية كافيا للحياة الشخصية، وللحريات والحقوق الأساسية. وقد حدد في المادة عينها، معايير تقييم مستوى الحماية الكافي، بالمقتضيات المعمول بها، وإجراءات الأمن التي تطبق، وخصائص المعالجة، مثل الغايات، والمدة، وطبيعة، واصل، ووجهة المعطيات المعالجة.

كذلك، أوردت المادة 44، بعض الحالات التي يجوز فيها نقل هذه البيانات، بالرغم من عدم توافر مستوى كاف للحماية، كالموافقة الصريحة للشخص المعني، والحالات التي يكون فيها النقل ضروريا، للمحافظة على حياة الشخص المعني، أو مصلحة عامة، أو احترام التزامات قانونية تتعلق بإحقاق العدالة، وحقوق الدفاع أمام المحاكم، والتعاون القضائي، أو الاتفاقات التي يكون فيها المغرب طرفا، وذلك، بناء على إذن صريح ومعلل، من اللجنة الوطنية.

وكان هذا القانون، قد أسند إلى هذه الأخيرة، مهمة إعداد لائحة بالبلدان، التي يتوافر فيها مستوى كاف للحماية، ومهمة إعطاء الإذن بنقل البيانات، بحسب منطوق المادة 43، المذكورة أعلاه.

وكذلك فعل المشترع الموريتاني، في الباب الخامس المعنون: "نقل المعطيات نحو بلد أجنبي"، والمشترع المصري، الذي خصص الباب السادس، "لحركة البيانات

خارج البلاد"، والمشترع التونسي، الذي خصص الباب الرابع، "لإحالة المعطيات الشخصية ونقلها". وقد اعتمدت هذه القوانين الأحكام عينها، والمبادئ نفسها.

وكان المشترع التونسي، قد نص على حظر نقل البيانات الشخصية، إلى بلاد أجنبية، في المادة 50، إذا كان من شأن ذلك المساس بالأمن العام، أو بالمصالح الحيوية للبلاد التونسية، فيما أوجبت المادة 52، الحصول على إذن من الهيئة، في كل حالات نقل البيانات إلى الخارج. وبما انه لا يمكن لمسؤول المعالجة، اتخاذ القرار حول طبيعة آثار هذا النقل، فانه لا بد وان يعود إلى الهيئة الوطنية، للحصول على إذن بذلك.

أما المشترع القطري، فقد حظر النقل عبر الحدود، في حال كانت معالجة البيانات مخالفة لأحكامه، أو إذا كان من شأنها الحاق ضرر جسيم بالبيانات الشخصية، أو بخصوصية الأفراد، على ما جاء في المادة 15، وهي المادة الوحيدة، التي تناولت إخراج البيانات الشخصية من الحدود الوطنية، في إطار إقرار حرية تدفق البيانات، عبر الحدود.

كذلك، لم يشر التشريع القطري، إلى شروط خاصة بمستوى الحماية، في البلد المتلقي لهذه البيانات، لكنه أورد أحكاماً عامة، حول التزامات المسؤول عن المعالجة، والمعالج، بضمان التطابق مع الأغراض المشروعة، وشروط المعالجة المشروعة، والأخطار الناجمة عن أي إخلال بالاحتياطات المفروض اتخاذها، لضمان سلامة البيانات، إذا كان من شأن هذا الأمر، أحداث ضرر جسيم بالبيانات، وبخصوصية الفرد.

ومن الواضح، أن حماية البيانات خارج الحدود، ليست محصنة كفاية في التشريع القطري، إذ إنها تفتقر إلى أحكام تقرر على أساسها إمكانية نقلها، أو حجبها، كما ورد في بقية القوانين. وبالتالي، سيعود للقضاء، وللسلطات المعنية، إيجاد الرد المناسب، في مواجهة التحديات، والخلافات، التي يمكن أن تظهر مستقبلا.

- الأشخاص المعنيون: الأشخاص الطبيعيون

من المهم التوقف عند هذا التعريف، لاسيما وأن الهدف الأساس، من قوانين حماية البيانات، هو حماية الأفراد، من مخاطر المعالجة الإلكترونية لبياناتهم الشخصية، سواء من قبل الدولة، أو من قبل الشركات، وما يمثله هذا الأمر، من إمكانات واسعة للاعتداء على الحريات والحقوق. وهذا، دليل واضح، على أن المعنيين بهذه الحماية، هم أشخاص طبيعيون.

لم تحدد الإرشادات الأوروبية لعام 1995، في المادة الثانية منها، والمخصصة للتعريفات، المقصود بهذا المفهوم. لكن عنوان الإرشادات[131]، أشار بوضوح إلى مجال تطبيقه، وهدفه: "حماية الأشخاص الطبيعيين، ...". كما أوردت الحيثيات، مرارا وتكرارا، عبارات تدل على شخص طبيعي، كالإنسان، والفرد، وممارسة الحقوق والحريات.

وهكذا، فإن الأشخاص المعنيين، هم كل شخص طبيعي، تجمع بياناته الشخصية، أو تحفظ، أو تعالج. وترتبط الحماية، والحقوق، والمبادئ، دون استثناء، بصفة الشخص المعني، أي صاحب البيانات. فإذا أخذنا بعين الاعتبار الأهداف، والحيثيات، وطبيعة الحقوق المحمية؛ كالحياة الخاصة، يمكن القول، أن الأشخاص المعنيون، ليسوا معنيين بهذه الإرشادات.

لكنهم في المقابل، يبقون معنيون باحترامها، كي لا يكونوا عرضة للعقوبات، التي تفرضها هذه القوانين، فيما لو خالفوا بعض أحكامها. وكذلك، يبقى الأشخاص الطبيعيون، أعضاء الشخص المعنوي، كالعاملين لديه، أو المدراء، معنيين لناحية استفادتهم، من حماية بياناتهم الشخصية.

[131] - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

ويمكن لأي شخص طبيعي، أن يصبح من الأشخاص المعنيين، بمجرد أن يبحر على الإنترنت، أو ينشر بياناته الشخصية عليها، أو على مواقع التواصل الاجتماعي، أو حين يقدم بطاقته الشخصية، أو يستعمل بطاقة اعتماد مصرفية.

وبالتالي، فانه يصبح معنيا، بأحكام قوانين حماية البيانات الشخصية، ويستحق ما تقره من حقوق، وفي مقدمها، حقه في عدم معالجة بياناته، إلا بإذن منه، من خلال إعطائه الموافقة على ذلك. وفي كل مرة، لا تكون هذه البيانات ضرورية لمن يقوم بجمعها، كي يستطيع إتمام موجب قانوني، يصبح الحصول على موافقة الشخص المعني، أمرا مطلوبا، وإلا اعتبرت المعالجة غير قانونية.

ومن مراجعة التعريفات الواردة في القوانين العربية، نلاحظ انسجامها، لهذه الناحية، مع الإرشادات الأوروبية. فجميع عناوينها، تحمل مصطلحات، تؤشر إلى شخص طبيعي، سواء باستخدام مصطلح مباشر، كحماية "الأشخاص الذاتيين"، في القانون المغربي، و حماية "الخصوصية"، و"البيانات الشخصية"، علما أن بعضها يستخدم مصطلح "حماية خصوصية البيانات". مع ملاحظتنا هنا، اللبس الذي يمكن أن ينتج عن هذا الأمر، لإنه يوحي بتمتع البيانات، بالحق في الخصوصية، علما أن هذا الحق، مرتبط بالشخصية الإنسانية.

وقد أوردت المادة السادسة من القانون التونسي، عبارة "المعني بالأمر"، والمقصود بها صاحب البيانات، على انه كل شخص طبيعي تكون معطياته الشخصية، موضوع معالجة. وكانت المادة الثانية من القانون المصري، قد اعتمدت التعريف نفسه، باستخدام مصطلح مختلف هو "الفرد"، وكذلك فعل القانون القطري، عندما خصص الفصل الثاني منه، لـ: "حقوق الأفراد"، في معرض إقرار حق الحماية،وغيره من الحقوق المتصلة به.

بالمقابل، غاب هذا التعريف عن القانونين المغربي والموريتاني، وان كان يمكن

استخلاص مضمونه من مصطلحات أخرى، مثل: "موافقة الشخص المعني"، حيث نجد نصا على قبول الشخص المعني، أو ممثله القانوني، بان تكون بياناته الشخصية، موضوع معالجة.

- **المسؤول عن المعالجة**

بحسب المادة الثانية، من الإرشادات الأوروبية، الصادرة عام 1995، يعرف المسؤول عن معالجة البيانات: ب "الشخص الطبيعي أو الاعتباري، أو السلطة العامة، أو المرفق، أو أية هيئة أخرى، تحدد بمفردها، أو بالاشتراك مع الآخرين، أغراض، ووسائل معالجة البيانات الشخصية"[132]. وكانت هذه المادة، قد تركت تعريف هذا المسؤول، إلى القوانين والأنظمة الوطنية.

لذا، يعتبر هذا المفهوم أصيلاً، ومستقلاً، من جهة أولى، بمعنى انه لا يمكن تفسيره، إلا في إطار قانون حماية البيانات، وذا مدلول وظيفي، من جهة ثانية، لإنه يهدف إلى تعيين المسؤوليات، بناء على دور الشخص، وتأثيره في عمليات المعالجة؛ أي على أساس واقعي، اكثر منه نظري، أو رسمي.

ويتمحور هذا التعريف، حول عناصر ثلاثة، مترابطة فيما بينها، هي: الطابع الفردي، من خلال استخدام عبارات: "الشخص الطبيعي، أو الاعتباري، أو السلطة العامة، أو المرفق، أو أية هيئة أخرى"، واحتمالات تعدد المسؤولية، من خلال: "بمفردها أو بالاشتراك مع الآخرين"، والعناصر الأساسية، التي تجعل من الممكن، التمييز بين الشخص المسؤول عن المعالجة، واللاعبين الآخرين؛ من خلال عبارة: تحدد أغراض ووسائل معالجة البيانات الشخصية".

[132] - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995- Article 2Définitions
- Aux fins de la présente directive, on entend par:
d) «responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire;
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

إن أول عناصر التعريف، وهو العنصر الشخصي، يؤشر إلى مروحة واسعة من الجهات، التي يمكن ان تلعب دور المسؤول عن المعالجة، بدءا من الشخص الطبيعي، وصولا إلى الشخص المعنوي، مرورا بأية جهة أخرى.

والمهم في التعريف، أن يضمن تطبيقا جيدا للقانون، عبر مساهمته قدر الإمكان، في تحديد المسؤول عن المعالجة، بشكل واضح لا لبس فيه، في جميع الظروف، حتى ولو لم يتم تعيينه قانونا، وبصورة رسمية. ويبقى أن الشخص المعنوي، أو المؤسسة، تبقى مسؤولة، عن احترام مبادئ حماية البيانات، وتنفيذ الموجبات، التي يفرضها القانون، حتى في الحالات، التي تلجأ فيها، إلى تعيين شخص طبيعي لديها، لمراقبة ومتابعة تنفيذ عملية المعالجة.

فالمبدأ الأساس، هو أن الشركة، أو الإدارة الرسمية، أو أية جهة أخرى، تبقى مسؤولة عن عمليات المعالجة، التي تنفذ في مجال نشاطها. ويكون الشخص الذي يعين مسؤولا، مجرد تابع للشخص المعنوي، يعمل بتوجيهاته، وتعليماته.

كانت اتفاقية 108[133]، قد لحظت مفهوم "رئيس الملف"، دون أن تخصه بدور أساسي. فقد نصت المادة الثانية منها، على عناصر تحديد المسؤول عن الملف، بوصفه الجهة المؤهلة لاتخاذ القرار، بشأن تحديد غايات المعالجة، وفئات البيانات الشخصية المعالجة، ونوعية العمليات التي ستخضع لها، مؤكدة في الوقت نفسه، على الحاجة إلى الأهلية القانونية، بنصها على توافق الأمر، مع القانون الوطني. وتكون بذلك، قد أحالت هذا التعريف، إلى القوانين الوطنية، حول حماية البيانات الشخصية، والتي يفترض بها، تحديد المعايير الخاصة، التي تعرف الجهة المؤهلة.

[133] - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Strasbourg, 28.I.1981 - Article 2 – Définitions Aux fins de la présente Convention:
d- «maître du fichier» signifie: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées.
https://rm.coe.int/1680078b39

إلا أن الصفة المستمدة من القانون، تم التخلي عنها، في إرشادات 1995، حيث اعتمد مفهوم الجهة التي تقرر، وسقط مفهوم الجهة المؤهلة بحسب القانون. وبذلك، لم يعد تحديد الجهة المؤهلة، بواسطة نص قانوني، إلزامياً، واصبح بإمكان أي كان، أن يعتبر مسؤولا عن معالجة البيانات، بعيدا عن أية صفة، أو مهمة رسمية، يحددها القانون. وهكذا يبرز تطور هذا المفهوم، ليصبح مفهوما اتحاديا، في إطار التوصيات الأوروبية، له مدلوله الخاص، بعيدا عن أي تحديد له، في القوانين الوطنية، وفي هذا الأمر، فرصة لتطبيق القانون بشكل أفضل، إذ تزال إمكانية اختلافه، بين بلد وآخر.

ومما لا شك فيه، أن لهذا الأمر دورا أساسيا، في اتخاذ المفهوم لبعد آخر، لم يكن له في اتفاقية، وفي تأمين تطبيق متجانس، ومنسجم، للإرشادات الأوروبية، على المستوى الوطني، في الدول الأعضاء في الاتحاد، من خلال إعطائها تفسيرا موحدا. ومن هذا المنظور، تابعت الإرشادات تطوير المفهوم، بنصها على استنتاج صفة المسؤول عن المعالجة، من خلال الحقائق والوقائع، التي تحيط بعمليات معالجة البيانات، ومن خلال الإجابة عن سبب القيام بها، وعن الشخص الذي يتولاها، بغض النظر عن وجود تحديد قانوني، بموجب نص صريح.

وبالتالي، لابد لإقرار صفة المسؤول عن المعالجة، من أن تقترن بقرار اتخذته جهة ما، للبدء بعملية المعالجة، تحقيقا لأهداف معينة، خاصة بها. وتكمن خطورة غياب هذا العامل، في إمكانية عدم انطباق القانون على الواقع؛ كالحالة التي ينص فيها على تعيين جهة ما كمسؤول عن المعالجة، فيما هي لا تقوم بذلك، حقيقة، لأنها تفتقر إلى السلطة التي تمكنها من تنفيذ مهمتها. أو كأن تسند الصفة قانونا، لجهة ما، تكون غير قادرة فعليا، على اتخاذ القرار، فيما يتعلق بأهداف المعالجة وغاياتها.

فقد يحدث، أن تعين جهة ما، شخصا بصورة رسمية، كمسؤول عن المعالجة، بينما يكون في الواقع، مجرد معالج، يعمل لصالح جهة أخرى، تتخذ القرار في تحديد الأهداف، والغاية، والوسائل.

ويمكن للإضاءة على أهمية هذا التحديد البراغماتي، الرجوع إلى ما عرف بقضية SWIFT[134]. فقد تم التعاقد مع هذه الشركة، بصفتها معالجا للمعلومات، بينما تبين في الواقع، إنها كانت تمارس صلاحيات المسؤول عن المعالجة، بسبب دورها الفعلي، في جمع البيانات، ومعالجتها، وإرسالها إلى جهات أمنية أميركية، تعالج هذه البيانات وتستخدمها في إطار عملية لمكافحة الإرهاب. وفي ذلك، تأكيد على صحة ما ذهبت إليه التوجيهات الأوروبية، لناحية اعتبار المسؤول، هو من يقرر الأهداف والوسائل، وليس من يعين قانونا.

ويطاول القرار حول وسائل المعالجة، القضايا التقنية، والتنظيمية، على السواء، والتي تترجم عمليا، بأجهزة الكومبيوتر، والبرامج المستعملة. كما يشمل أيضا، العناصر الأساسية لعملية المعالجة، والتي تحفظ تقليديا للمسؤول عن المعالجة، مثل نوعية البيانات التي ينبغي معالجتها، ومدة الاحتفاظ بها، وأصحاب الحق في الوصول إليها. لكن لا بد من الإشارة هنا، إلى احتمال أن يقوم المعالج، باتخاذ القرار في تحديد الوسائل، دون أن يؤثر هذا الأمر، على تحديد صفة المسؤول عن المعالجة، حيث يبقى هذا الأخير، صاحب قرار تحديد أهداف المعالجة، وغاياتها.

ومن زاوية حماية البيانات الشخصية، يتم تحديد المسؤول عن المعالجة، في الواقع، بالاستناد إلى قواعد القانون المدني، أو الجزائي، أو الإداري، التي تحكم تحديد المسؤوليات، أو إنزال العقوبات، بحق شخص طبيعي، أو شخص معنوي. ولا

---

[134] - Le transfert de données bancaires à caractère personnel vers les Etats-Unis : aspects juridiques de l'Affaire SWIFT- Master 2 Professionnel Droit de l'Internet Public Administration – Entreprises Présenté et soutenu publiquement Par Richard MONTBEYRE
http://www.droit-tic.com/pdf/Aspects-juridiques-Swift.pdf

تطرح المسؤولية المدنية، كما هو معروف قانوناً، أي إشكال على هذا المستوى، لإنها تطبق على الأشخاص المعنويين، كما تطبق على الأشخاص الطبيعيين. بينما تنص بعض الأنظمة القانونية، على إقرار المسؤولية الإدارية، أو الجزائية، بحق الأفراد الطبيعيين، حصرا.

وفي هذا الإطار، لا بد لقوانين حماية البيانات الوطنية، التي تلحظ عقوبات إدارية، أو جزائية، أن تأخذ هذا الواقع بعين الاعتبار، بحيث تنزل العقوبة في هذه الحالة، بحق موظفي الأشخاص المعنويين، بحسب قواعد خاصة، يلحظها القانون، لهذه الغاية. ويمكن لهذا الأمر، أن يستند إلى الصفة التمثيلية، التي يتمتع بها الموظف، وإلى صلاحيته في اتخاذ القرارات، باسم الشخص المعنوي، إضافة إلى سلطته على ممارسة السيطرة، واتخاذ القرار، ضمن هيكلية الشخص المعنوي.

بالانتقال إلى العنصر الآخر في التعريف، أي الانفراد أو الاشتراك في معالجة البيانات، فقد لحظت الإرشادات الأوروبية، واقع تدخل عدد من الجهات، بصفة مسؤول عن المعالجة، فيما لم يكن هذا الواقع قد أخذ بعين الاعتبار، في اتفاقية 108. ويعتبر هذا الأمر ضروريا، عندما يتخذ قرار معالجة البيانات، وتحدد أهدافها، ووسائلها، بالاشتراك بين عدد من الجهات. ففي هذا الوضع، تعتبر كل جهة منهم، مسؤولة عن المعالجة، تجاه الأشخاص المعنيين، بمعنى انه يمكن لهم مراجعتها، في كل ما يتعلق بحقوقهم، في إدارة هذه البيانات.

فمن الشائع أن يعمد عدد من الجهات، إلى العمل معا على معالجة البيانات، كجهات مسؤولة عن المعالجة، وهي حالة لم يستبعدها التعريف الوارد، في الإرشادات الأوروبية. فقد عددت هذه الأخيرة، المراحل، والعمليات، التي يمكن أن يتم تنفيذها، من قبل جهات مختلفة، بشكل متلاحق، أو متزامن، وصولا إلى معالجة البيانات، ما يمكن أن ينتج عنه، مسؤولية مشتركة، في كل مرة، تشترك فيها

جهات مختلفة، على تحديد أهداف عملية معالجة بيانات، والوسائل المستخدمة لتنفيذها، والغايات المحددة من نتائجها.

والمثل الذي يمكن سوقه هنا، هو الشبكات الاجتماعية، التي تلجأ إلى إنشاء منصات مشتركة، تتيح لمستخدميها تبادل المعلومات، والتواصل فيما بينهم. ويعتبر مزودو الخدمة هؤلاء، مسؤولين عن معالجة البيانات، لإنهم يشتركون في تحديد أهداف المعالجة، والوسائل التي تستخدم لهذه الغاية.

وبالرجوع إلى عدد من القوانين الأوروبية، نجد أن المسؤول هو الشخص الذي يحدد أغراض، ووسائل معالجة البيانات الشخصية. وبالتالي، إذا قررت شركة ما، أو أية مؤسسة، "لماذا" و"كيفية" معالجة البيانات الشخصية، فستكون هي المسؤول عن المعالجة. ويكون الموظفون العاملون على تنفيذ عملية المعالجة، هم المعالجون.

من جهتها، عرفت القوانين العربية، دون استثناء، المسؤول عن المعالجة، أو المراقب، معتمدة المعايير نفسها، التي أخذت بها التوجهات الأوروبية، مع اختلافات بسيطة، لناحية التوسع، في الإشارة إلى ضرورة تحديد المسؤول عن المعالجة، في حالة تحديد غايات المعالجة، ووسائلها، بواسطة نصوص تشريعية، أو تنظيمية[135]. وقد استخدم القانونان المصري والقطري، مصطلح "المراقب"، وهذه الصفة، مأخوذة كما هو واضح، من دوره في متابعة، وملاحقة، تنفيذ عمليات المعالجة، سواء منها تلك التي تجري مباشرة من قبل تابعين له، يعملون ضمن إطار مؤسسته، أو من قبل متعاقدين معه، من خارج هذه المؤسسة.

في المقابل، اعتمدت قوانين تونس، والمغرب، وموريتانيا، عبارة "المسؤول عن المعالجة"، وهي أكثر شمولية، لجهة المهام المطلوبة من هذا الشخص، على ضوء الالتزامات التي ينص عليها القانون. لكن هذا الاختلاف، يبقى اختلافا لغوياً، لا

---

[135] - الفقرة 5 من المادة الأولى، من القانون المغربي 09.08 حول حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي

يؤثر في فاعلية الأحكام وتطبيقها، بشكل خاص، لناحية تحديد المسؤوليات.

- **المتعاقد من الباطن**

لم تلحظ اتفاقية 108، دور المعالج، أو المتعاقد مع المسؤول عن المعالجة، ولم يدخل مصطلح "المعالج، أو المتعاقد من الباطن، إلى الإرشادات الأوروبية 1995، كمفهوم واضح ومستقل، إلا بناء على اقتراح البرلمان الأوروبي[136]. وعلى غرار مفهوم المسؤول عن المعالجة، يشمل هذا المفهوم، مروحة واسعة من الجهات، التي يمكن اعتبارها مسؤولة عن المعالجة. ويعود لهذا الأخير، إقرار وجود المعالج، عندما يختار أن يوكل عددا، أو جميع عمليات المعالجة، إلى جهة ثالثة، تعمل لحسابه، لكنها تتمتع باستقلال قانوني عنه، وخارجة عن إطار مؤسسته.

وكانت المادة الثانية [137]من الإرشادات، قد نصت على اعتبار أية هيئة، أو شخص طبيعي، أو معنوي، أو إدارة رسمية، تعالج البيانات الشخصية، لحساب مسؤول عن المعالجة، بمثابة المتعاقد من الباطن.

تأسيساً على ما تقدم، تتوافر صفة المعالج، في الجهة التي تتمتع باستقلال كيانها القانوني، عن المسؤول عن المعالجة، وحيث تقوم بالمعالجة لحساب هذا الأخير. وقد تنحصر عملية المعالجة، في مهمة محددة، أو سياق معين، أو قد تكون عامة وواسعة. بالإضافة إلى ذلك، لا يتحدد دور المتعاقد من الباطن، لدى اللجوء إلى "الاستعانة بالمصادر الخارجية"، من طبيعة الكيان الذي يقوم بالمعالجة، بل من الأنشطة الملموسة، التي ينفذها ضمن إطار محدد.

---

[136] - Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)
https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52012PC0011

[137] - Article 2
Définitions Aux fins de la présente directive, on entend par:
e) «sous-traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

بعبارة أخرى، يمكن أن يعمل المتعاقد من الباطن، كمسؤول عن المعالجة، في إطار عمليات معينة، وكمعالج في إطار عمليات أخرى. ويتم تحديد هذا الأمر، بناء على مجموعة عناصر، تتكون من مجموعة بيانات، أو مجموعة أنشطة.

ويعتبر مزود خدمات الإنترنت، الذي يقدم خدمة استضافة البيانات، من حيث المبدأ، متعاقدا من الباطن، بالنسبة لتعامله مع البيانات الشخصية، التي ينشرها زبائنه على الإنترنت، والذين يلجأون إلى خدماته كمضيف، وكمسؤول عن صيانة مواقعهم. لكن الأمر يختلف، في حال قيام مزود الخدمات هذا، بمعالجة البيانات الشخصية المذكورة، لأغراض شخصية، يحددها هو، حيث يتحول إلى "مسؤول عن المعالجة"، بالنسبة إلى هذه العملية، تحديدا. وهنا يبدو واضحا، أن الشرط الخاص، بان يعمل المتعاقد من الباطن، لمصلحة صاحب الموقع، أي المسؤول عن المعالجة، وليس لمصلحته الخاصة، هو ما يعرف قانونا، بالتفويض.

فبحسب تشريع حماية البيانات الشخصية، أن المتعاقد من الباطن، ينفذ تعليمات المسؤول عن المعالجة، أقله ما يتعلق منها، بتحديد أهداف المعالجة، والعناصر الأساسية لوسائلها. علما، أن القانون يترك لهذا المتعاقد، بعض الحرية في اختيار الوسائل الأنسب، باعتباره مفوضا، يعمل لخدمة مصلحة شخص ثالث، هو من فوضه، وعليه أن يؤدي هذه الخدمة، بأفضل طريقة ممكنة. ويكون السند القانوني الذي يعطي عمله مشروعيته، الولاية التي يمنحه إياها المسؤول عن المعالجة. فإذا تجاوز حدود التفويض الممنوح له، وقام بالمعالجة لأغراض، وأهداف خاصة به، أو مختلفة عن تلك المحددة أساسا لعملية المعالجة، يصبح نشاطه غير قانوني.

وكانت الإرشادات الأوروبية، قد حددت في المادة 17 منها[138]، شروطا خاصة بالمتعاقد من الباطن، تضمن الحفاظ على المستوى المطلوب لحماية البيانات، عندما يختار المسؤول عن المعالجة، أن يوكل مهمة التنفيذ،إلى جهة ثالثة. وقد أقرت لهذه الغاية، ضرورة إلزام المسؤول عن المعالجة، باختيار متعاقد من الباطن، يقدم ضمانات كافية، فيما يتعلق بأمن البيانات، على المستويين التقني والإداري، لجهة المعالجة المنوي تنفيذها، على أن يسهر على الالتزام بهذه الضمانات.

كما نصت المادة نفسها، على ضرورة تنظيم عقد، أو أية وثيقة قانونية ملزمة، يلحظ فيها، قيام المتعاقد بتنفيذ المعالجة، بحسب تعليمات المسؤول عنها، حصرا، إضافة إلى التزامه بجميع الموجبات الملقاة على عاتق هذا الأخير. علما أن المادة 16[139]، التي تنص، على سرية المعالجات، منعت كل من يعمل تحت سلطة المسؤول عن المعالجة؛ كالمتعاقد من الباطن، والأشخاص الذين يعملون تحت سلطة هذا الأخير، ويصلون إلى البيانات الشخصية، من معالجتها، إلا بناء على تعليمات المسؤول عن المعالجة.

من جهتها، لحظت القوانين العربية، بالنسبة لتعريف المعالج، وجوب الأخذ بعين الاعتبار، عنصر "تنفيذ العمل لصالح المسؤول عن المعالجة. فاستخدم التشريع التونسي، مصطلح "المناول"، والموريتاني، "المعالج الوسيط"، والمغربي، "المعالج من الباطن"، والقطري والمصري، "المعالج". وقد أفردت مواد خاصة، لحظر معالجة

---

[138] - Art. 17
2. Les États membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures.
3. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:
- Le sous-traitant n'agit que sur la seule instruction du responsable du traitement,
- Les obligations visées au paragraphe 1, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci.
4. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 1 sont consignés par écrit ou sous une autre forme équivalente.
https://www.gdpr-expert.eu/article.html?id=29#textesofficiels

[139] - Article 16- Confidentialité des traitements
Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

البيانات، دون تعليمات المسؤول، ما لم تفرض ذلك، التزامات قانونية[140].

وأفرد القانون المصري، في الباب الرابع، أحكاماً خاصة بالتزامات المعالج، قرنها بالتزامات المراقب، ونص فيها، على ضرورة وجود عقد، ينظم عملية المعالجة من الباطن، وبشكل خاص، فيما يتعلق بكونها، تنفذ بناء على تعليمات المسؤول عن المعالجة، وبموجب إجراءات تقنية، وتنظيمية، تضمن حماية البيانات من التلف، والضياع، والتسرب، وجميع أشكال المعالجة غير المشروعة، عندما تستوجب المعالجة إرسال البيانات، عبر شبكة معينة.

- **الشخص الثالث / الغير/ الأغيار**

أن الغير، أو الجهة الثالثة، مصطلح قديم، يراد به التدليل، على مبدأ قانوني، يقضي باقتصار مفاعيل العقود والأحكام القضائية، على أطرافها، سواء أكان ذلك، لنفع أو لضرر. وقد اعتمد هذا المصطلح، في القوانين المدنية، ومن قبل الاجتهاد، دون أن يتم تخصيصه بتعريف، من خلال نص قانوني محدد.

إلا أن المصلحة الخاصة، لهذا الغير، استدعت محاولات من الفقه، والباحثين، لتحديد أطره، ومدلوله، لاسيما مع التحولات الاقتصادية والتقنية، وما رافقها من تطور مفاهيم ونظريات قانونية، لاسيما في المجالات الاقتصادية، والتقنية، والصناعية، والتجارية، بهدف تنظيم العلاقات بين أطراف معينة، وقد أوجب هذا الأمر إخراج من ليس طرفا فيها، إلى إطار قانوني مختلف.

فقد ورد مصطلح "الغير"، في القانون، في إطار مبدأ نسبية العقود، وفي مجال العقود الصورية، والتأمين الإجباري في المسؤولية المدنية، عن حوادث السير. أما الفكرة الأساس منه، فهي حماية استقرار المعاملات القانونية، واستقرار العلاقات في المجتمع، وحماية من اعتمدوا عن حسن نية، على تصرف توافرت له مظاهر

[140] - المادة 27 من القانون المصري، المادة 25 من القانون المغربي.

التصرف القانوني الصحيح، لاسيما وان صورية العقود، قد تستخدم أحيانا، كوسيلة للاحتيال على القانون، وتهربا من إلزاماته؛ كعقد البيع، الذي يخفي هبة.

ويمكن للعقد أن يكون لمصلحة الغير، كما هو الحال، في مجال التأمين، حيث يجرى العقد لحماية المتضررين المستقبليين، والاحتماليين، من الحوادث. وغني عن القول، إن هذا الحق للغير، في الإفادة من علاقة عقدية، لم يكونوا طرفا فيها، ينشأ بحسب مبدأ سلطان الإرادة، الذي يتيح التعاقد لمصلحة الغير، بموجب وثيقة التأمين. ويعطي عقد التأمين، الحق للمتضرر بالرجوع، على شركة التأمين، لمطالبتها بالتعويض عن الأضرار التي لحقت به.

إذا، وبحسب القانون المدني، يمكن القول أن الشخص الثالث، هو كل شخص طبيعي، أو معنوي، خارج عن إطار العقد، أو المؤسسة، أو الخصومة في الدعاوي القضائية.

وتكمن أهمية تحديد فئة الأشخاص الثالثين، أو "الأغيار"، في قانون حماية البيانات الشخصية، بحسب الحيثيات التي وردت، في تعديل الإرشادات الأوربية 1995، في كونها تساعد على استبعاد فئات "الشخص المعني"، و"المسؤول عن المعالجة"، و"المتعاقد من الباطن"، أو من يعمل لحسابهما، من إطارها. فموظفو وكالة السفر، التي تعالج البيانات الشخصية لزبائنها، ليسوا جهة ثالثة، بينما يعتبر العاملون لمؤسسة أخرى، كذلك، وان كانت هذه الأخيرة، مملوكة للمجموعة نفسها، صاحبة وكالة السفر.

وقد استخدمت الإرشادات، عبارة "الشخص الثالث"، أو "الغير"، بطريقة مشابهة، لتلك التي وردت في القانون المدني، أي الشخص الذي لا علاقة له بالعقد، أو بالكيان (المؤسسة، المنظمة، الإدارة). وهكذا يكون المقصود من ورود هذا المصطلح، في إطار حماية البيانات، كل شخص لا يملك إذناً خاصا، أو حقا

مشروعا، لمعالجة البيانات الشخصية. وغالبا ما استخدم المصطلح، في سياق الحظر، وتحديد الصلاحيات، والمسؤوليات، في حال سلمت معالجة البيانات، إلى جهة لم تكن في الأساس، معنية بهذه المعالجة.

وهكذا، يمكن أن يتحول الشخص الثالث، أو "الغير"، الذي تلقى البيانات بصورة مشروعة، أو غير مشروعة، إلى "مسؤول عن المعالجة"، كلما توافرت عناصر تحديد هذه الصفة، ويصبح، بالتالي، خاضعا لأحكام قانون حماية البيانات.

وبالفعل، عرفت بعض القوانين العربية، هذه الفئة، نسبة إلى علاقتها، ودورها بمعالجة المعلومات، فاستبعدت منها، "الشخص المعني"؛ أي صاحب البيانات المعالجة، والمستفيد من المعالجة، والمسؤول عنها، والمنفذ لها؛ كالمتعاقد من الباطن، أو المناول بحسب القانون التونسي، الذي اعتمد مصطلح "الغير"، واعتمد القانون المغربي، المصطلح نفسه في صيغة الجمع، أي "الأغيار"، بينما لم يتطرق إلى تحديدها، أي من المشترع القطري، أو المصري، أو الموريتاني.

المبادئ: مرتكز الحقوق والموجبات

تعتبر المبادئ، التي تقرها قوانين حماية البيانات الشخصية، المصدر الأساس، لحقوق الشخص المعني، وموجبات المعالج، وكل من هو معني بالوصول إليها، أو بعملية المعالجة.

من هنا، لا بد بداية من استعراض هذه المبادئ، كما وردت في القوانين الأوروبية، وتوصيات الجهات الدولية.

وترتكز قوانين الحماية، بشكل أساسي، على فلسفة احترام مبادئ حقوق الإنسان، وضمان حماية الحق في الخصوصية، وإقرار آليات تضمن تحقيق أهدافه، من ضمن هذه الفلسفة. وعليه، كان لا بد من الالتفات إلى ضمان سلامة عملية المعالجة، عبر إقرار عدد من المبادئ، التي تلزم المسؤول عن المعالجة، كمشروعية المعالجة،

وشفافيتها، وأمانتها، ونزاهتها، وضرورتها. وفي هذا السياق، حظرت القوانين معالجة البيانات الشخصية، بطريقة تمس بحقوق أصحابها، أو بحرياتهم الخاصة والعامة، أو تسيء اليهم، وتشهر بهم.

وفي هذا الإطار، أقرت القوانين الخاصة بحماية البيانات الشخصية، بصورة عامة، والقوانين العربية، بصورة خاصة، عددا من المبادئ، التي يفترض بالمسؤول عن المعالجة احترامها، كي لا تنتج عنها أي إساءة إلى أصحاب البيانات، وفي مقدمها، مبدأ الشفافية، وتوفير الإعلام الكافي عن عملية المعالجة، إضافة إلى ضرورة إتاحة فرصة لصاحب البيانات، كي يتمكن من ممارسة حقوقه.

إلا أن الأحكام الخاصة بالمبادئ والموجبات، تداخلت، واختلف تنظيمها بين تشريع وآخر. ويمكن فهم هذا الأمر، انطلاقا من اعتبار المبادئ، القاعدة الأساسية، التي تقرر موجبات المسؤول عن المعالجة، ومنفذها، والجهات الخارجية المتعاقدة مع المسؤول، بهدف تنفيذها. كما اختلفت القوانين، لناحية إعطاء تفاصيل، أو إقرار مبدأ عام، يمكن تفسيره بناء على فلسفة القانون، وأهدافه.

فقد أورد المشترع المصري، مبادئ المعالجة، في المادة الرابعة المعنونة: "جودة البيانات"، من الباب الثاني، الذي حمل عنوان: "حقوق الأفراد"، بينما وردت في التشريع المغربي، في المادة الثالثة، في الفرع الثاني، المعنون: "نوعية المعطيات والرضى المسبق للشخص المعني"، وأوردها التشريع القطري، في المادة الثامنة، من الفصل الثالث، الذي حمل عنوان: "التزامات المراقب والمعالج"، وتطرق إليها المشترع التونسي، في المواد التاسعة، والعاشرة، والحادية عشرة، من القسم الثاني، وعنوانه: "في المسؤول عن معالجة المعطيات الشخصية وواجباته".

أما المشترع الموريتاني، فقد تميز بتخصيص الفصل الثاني من القانون، لهذا الأمر، وذلك من المادة 5 إلى المادة 31، مقسما إياه إلى أربعة أجزاء، وزعت عليها

المبادئ، تبعا لطبيعة البيانات، والعمليات التي تطاولها. وقد جاءت عناوينها، على الشكل التالي:

"المبادئ القاعدية المتعلقة بمعالجة البيانات ذات الطابع الشخصي"، "المبادئ الخاصة بمعالجة بعض فئات البيانات ذات الطابع الشخصي"، "المبادئ الخاصة بتحويل البيانات ذات الطابع الشخصي إلى بلد آخر"، و"الربط البيني للملفات التي تحتوي على بيانات ذات طابع شخصي".

وقد تضمنت جميع النصوص العربية، مبدأ الهدف المعلن، والمحدد، والمشروع، والالتزام بالغاية طوال مدة المعالجة، مع التشديد على تنفيذ العملية، في إطار الشفافية، والنزاهة، واحترام كرامة الإنسان، والممارسات المقبولة قانونا. كما أقرت مبدأ الملائمة، وتناسب البيانات مع هدف المعالجة، وعدم الإفراط في جمعها، نسبة إلى الأهداف المرجوة من عملية الجمع، وصحتها، ودقتها، واتخاذ الإجراءات المناسبة لأرشفتها، أو إتلافها، بعد الانتهاء من تحقيق الهدف، إضافة إلى مبدأ عدم جواز الاحتفاظ بالبيانات، لفترة غير محددة، وعدم جواز جمعها، بطرق ملتوية، ومخالفة للقانون، أي دون علم صاحبها، ودون إعلامه.

- **الهدف الواضح، المحدد والمشروع**

يجب أن تكون أغراض المعالجة واضحة، ومحددة، ومشروعة، ومحترمة طوال فترة استمرار العملية، واستخدام المعلومات، والاحتفاظ بها. كما لا يجوز استخدام البيانات المحفوظة، لأهداف أخرى غير تلك التي يتم الإعلان عنها. ويسمح تحديد الهدف، بمعرفة البيانات الضرورية لعملية المعالجة، ونوعيتها.

فلا يجوز، على سبيل المثال، استخدام البيانات التي جمعت لإدارة شؤون الزبائن، بهدف توجيه إعلانات تسويقية اليهم. ولا بد من أن تكون الأهداف المحددة، منسجمة مع طبيعة عمل المؤسسة المسؤولة عن المعالجة، ومهماتها. والمثال الذي

يمكن تقديمه هنا، هو تحسين نوعية الخدمات، وإدارة شؤون الموظفين، والعملاء، والزبائن، وإجراء استطلاعات رأي حول نوعية الخدمات، وحماية المصالح المالية للشركة.

ففي عملية معالجة ملفات زبائن وكالة نقليات، لا يمكن تخيل سبب يستدعي طلب رقم بطاقة الضمان الصحي من الزبون، أو معلومات عن محيطه العائلي، والمهني. كما يسمح تحديد الهدف، بتحديد مدة الاحتفاظ بالبيانات، إذ يفترض محو معلومات الأشخاص، الذين تركوا عضوية ناد، أو جمعية، أو تركوا المؤسسة، إلا متى كان هذا الأمر ضروريا، لحاجات إثبات قانونية، تفرضها القوانين المرعية الإجراء.

- **ملاءمة البيانات**

لا يجب أن تستخدم المعلومات المعالجة، إلا للهدف الذي حدد في وقت جمعها، بحيث لا تجمع إلا البيانات التي تخدم الوصول إلى هذا الهدف، بصورة حصرية.

وكما يفترض الحرص، على عدم جمع البيانات بطريقة مبالغ فيها، ولا حاجة لها في خدمة الهدف، كذلك يفترض الحرص، على عدم جمع البيانات التي تعتبر حساسة، والتي تمنع معالجتها، إلا بصورة استثنائية، بموجب إجراءات إدارية خاصة، ولأهداف محددة قانونا.

إلا انه يمكن معالجة هذه البيانات، فيما لو كانت قد نشرت بصورة عامة، ووضعت في متناول الجمهور، أو في حال موافقة صريحة، وخطية، ومحددة، من صاحبها، أو بهدف الحفاظ على حياة إنسان، أو كان استخدامها مرخصا به، بحسب القانون، خدمة لمصلحة عامة، أو كان أصحابها أعضاء في جمعيات أو مجموعات عرقية، أو سياسية، أو دينية، أو أثنية. ويضاف إلى ذلك، ضرورة الانتباه إلى المعلومات المتعلقة بالجنايات والجرائم، والتي تنظم معالجتها، ضمن اطر قانونية خاصة.

وقد أشارت كل من المحكمة الأوروبية لحقوق الإنسان، ومحكمة العدل الأوروبية، إلى هذا المفهوم، في العديد من قراراتهما، بحيث اعتبر التدخل في الحياة الخاصة ممكنا، ومقبولا، في كل مرة، يتوفر فيها مبدأ الملاءمة، الذي يمكن قياسه بناء على مدى توازنه مع مشروعية هذا التدخل، ومبرراته المشروعة، (كالمصلحة العامة)، وأساليبه. فالتنصت الهاتفي، الذي لم يلحظه القانون، لا يعتبر تدخلا مشروعا، والمبررات غير الواضحة، التي تقدم، لا يمكن الأخذ بها[141].

وفي السياق عينه، اعتبرت محكمة العدل الأوروبية، أن الرقابة على المالية العامة، لضمان استخدام الاستعمال الأمثل للأموال العامة، تشكل هدفا مشروعا يبرر التدخل في الحياة الخاصة، عبر معالجة البيانات الشخصية[142].

ويمكن هنا، استخلاص عناصر قياس الملائمة، التي أقرت اجتهادا، وبناء على النصوص التي تمنع، أو تسمح بالتدخل في الحياة الخاصة، بضرورة وجود نص قانوني يجيز التدخل، وبضمان عدم تأثير هذا الأخير، على احترام الحق الأساسي في الحياة الخاصة، وحصر هدف التدخل في تحقيق المصلحة العامة، إضافة إلى

---

[141] - Malone contre Royaume-Uni- 2 Aout 1984 Req. 8691/79 - les données communiquées à la Cour ne permettent pas de dire avec l'assurance souhaitable à quels égards le pouvoir d'interception se trouve intégré à des normes juridiques et sous quels rapports il reste tributaire de l'exécutif. En raison de l'ambiguïté et de l'incertitude qui subsistent sur cet aspect capital du droit en vigueur, la Cour ne saurait arriver à une conclusion différente de celle de la Commission. A ses yeux, le droit anglais et gallois n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. Dans cette mesure fait défaut le degré minimal de protection juridique voulu par la prééminence du droit dans une société démocratique. - 80. En résumé, les atteintes au droit du requérant au respect de sa vie privée et de sa correspondance (paragraphe 64 ci-dessus), tel que le garantit l'article 8 (art. 8), n'étaient pas "prévues par la loi" pour autant qu'il s'agit de l'interception de communications.
https://www.doctrine.fr/d/CEDH/HFJUD/CHAMBER/1984/CEDH001-62091

[142] - 10. CONCLUSIONS DE L'AVOCAT GÉNÉRAL M. ANTONIO TIZZANO
présentées le 14 novembre 2002 (1)Affaire C-465/00RechnungshofcontreÖsterreichischer Rundfunk e.a.
L'article 7 détermine ensuite les cas dans lesquels «le traitement de données à caractère personnel [...] peut être effectué», en précisant, pour ce qui nous occupe, que le traitement est permis lorsqu'il est nécessaire «au respect d'une obligation légale à laquelle le responsable du traitement est soumis» ou «à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées».
11. Il convient en outre de rappeler que l'article 13 autorise les États membres à déroger à certaines dispositions de la directive, et notamment à l'article 6, paragraphe 1, si cela est nécessaire pour sauvegarder, entre autres, «un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal» [point e)] ou «une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique» dans des cas particuliers au nombre desquels figure celui visé au point e) qui vient d'être évoqué [point f)].
http://curia.europa.eu/juris/document/document.
jsf?text=&docid=47891&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=697205

ملائمة الحق في الحد من الحق في حماية الحياة الخاصة، مع الهدف المرجو منه، بمعنى أن يكون من شأنه المساهمة في تحقيق الهدف، وإلا يتجاوز التدخل، ما هو مناسب وضروري لذلك.

وغني عن القول، أن المصلحة العامة، التي تشكل حدودا للحق في الحياة الخاصة، تمثل في معظم نشاطات السلطة العامة، والتي تمارسها في مجالات مكافحة الجريمة، ومواجهة الإرهاب، وملاحقة الجرائم الخطرة، والحفاظ على استقرار وأمن المجتمع.

- **تحديد مدة حفظ المعلومات**

تتأثر مدة حفظ المعلومات، مباشرة بالهدف المرجو من عملية المعالجة. كما تتأثر بمبدأ الملائمة، الذي يفرض جمع البيانات الضرورية، واللازمة فقط.

وعليه، لا يمكن الاحتفاظ بالمعلومات الشخصية، لفترة غير محددة. لذا يفترض بالمسؤول عن المعالجة، أن يحدد هذه المهلة، على ضوء طبيعة المعلومات، والهدف من معالجتها، بحيث يتم محوها، أو إتلافها، أو تشفيرها، أو أرشفتها، عند تحقيقه.

لذا تختلف مدة الاحتفاظ بالمعلومات التي تجمع عن الموظفين، عن تلك التي تجمع عن زوار المباني؛ بهدف الحفاظ على الأمن، ومراقبة مداخل الابنية، أو تلك التي تجمع في المجال الطبي، لمتابعة المرضى، أو لدراسة انتشار الأوبئة، ومفعول العلاجات.

ذلك، تستقل حدود مدة الاحتفاظ بالبيانات عن زمن تحقيق الهدف، في كل مرة، لا يكون ممكنا تحديد وقت الإفادة منها، كأن تكون هذه البيانات وسيلة إثبات علاقات عمل، أوالتزامات، أو عقود.

فانحلال الشركة، أو إعلان إفلاسها، لا يحتم إتلاف البيانات الشخصية لمديريها، أو لمن تولوا أعمال التصفية، إذ يمكن أن تكون هنالك حاجة إليها، في قضايا تتعلق

بحماية مصالح الشركاء، أو المساهمين، أو الأشخاص الثالثين، أو أصحاب العقود معها. لكن ذلك، لا يمنع أصحاب البيانات، من ممارسة حقهم في الاعتراض، عندما يرون أن الاحتفاظ ببياناتهم، لم يعد يخدم تحقيق الهدف المرجو، أساسا. ويبقى للمحكمة اتخاذ القرار المناسب، على ضوء كل حالة.

ويعتبر تحديد مدة حفظ المعلومات، إضافة إلى الحق في طلب التعديل، المرتكز الأساسي، للحق في المحو، الذي مهد بدوره، لإقرار الحق في النسيان، عبر محو البيانات الشخصية، في القواعد الأوروبية الجديدة لحماية البيانات الشخصية

- **محو البيانات**

كانت الإرشادات الأوروبية الصادرة عام 1995، قد نصت في المادة 12 منها، على ضرورة ضمان حق كل شخص، في طلب محو بياناته الشخصية، وعلى موجب يترتب على المسؤول عن المعالجة، بتلبية هذا الطلب، في حال كانت معالجة البيانات، مخالفة لأحكام الإرشادات، بسبب نقصها، أو عدم صحتها. كما فرضت على المسؤول، إبلاغ الجهات الثالثة، التي نقلت إليها البيانات، عن كل تعديل، أو محو، أو تجميد، ما لم يكن الأمر يتطلب جهدا غير متناسب، أو مستحيلا.

وكانت الهيئة الوطنية الفرنسية للمعلوماتية والحريات، قد وضعت لائحة بعدد من المعايير[143]، التي يجب العودة إليها، لتقدير الاستجابة لطلب المحو. وتعتبر هذه المعايير غير حصرية، بحيث يمكن تطويرها، على ضوء الخبرة المكتسبة.

أما اعتمادها، فقد تم بناء على عدد من العوامل الشخصية، كسن مقدم الطلب، ومركزه الاجتماعي والسياسي، والمهني، من جهة، وعلى طبيعة البيانات، ودقتها، وشرعيتها، من جهة ثانية، إضافة إلى مدى تأثيرها في الحاق الضرر بصاحب البيانات، أو في ممارسة أفراد المجتمع لحقوقهم في الاستعلام، وفي الوصول إلى

[143] - https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf

المعلومة. ويمكن تلخيص هذه المعايير، على الشكل التالي:

يقتصر مجال تطبيق الحق في طلب المحو، على اسم العلم، أو الاسم المستعار للشخص المعني، عندما تكون نتائج البحث عائدة لشخص طبيعي، أو في حال استخدام الاسم، أو الاسم المستعار، كمفاتيح للبحث. إلا أن هذا الأمر لا يعتبر مبررا كافيا، عندما يكون الشخص المعني، من الشخصيات التي تلعب دورا في الحياة العامة؛ كأن يكون زعيما سياسيا، أو صاحب منصب وزاري، أو برلماني، وعلى أن تؤخذ طبيعة المعلومة بعين الاعتبار، بحيث يفترض التمييز، بين المعلومة المرتبطة بحياته العامة، وتلك المرتبطة بحياته الخاصة.

ويصبح الالتزام بموجب احترام طلب الحذف، اكثر صرامة، متى كان الشخص المعني قاصرا، انطلاقا من مبدأ تفضيل مصلحة الطفل، على أية مصلحة أخرى، وذلك بناء على ميثاق الحقوق الأساسية للاتحاد الأوروبي.

في حال كانت البيانات المطلوب محوها مغلوطة، يفترض الاستجابة فورا لطلب الحذف، على أن يقوم طالب المحو، بتقديم الإثبات على ذلك، إلى الهيئة الوطنية، المسؤولة عن متابعة مسائل حماية البيانات الشخصية. أما في حال البيانات المفرطة، أو المعتبرة غير ذات صلة، فلا بد من التمييز بين كونها خاصة بالحياة المهنية، أو بالحياة الخاصة، إذ لا يتوجب الالتزام بحذف الأولى، كون الحق في المحو، يهدف إلى حماية الحياة الخاصة، وليس إلى إخفاء ممارسات خاطئة، من حق الجمهور الاطلاع عليها.

كذلك، لا يمكن حذف المعلومات، التي تشكل تشهيرا، أو إهانة، أو افتراء، إلا بناء على حكم قضائي، أو بناء على قرار من الهيئة الوطنية لحماية البيانات الشخصية، يكون مبنيا على طبيعتها المفرطة. وهنا أيضاً، يجب التمييز بين كون المعلومات تشكل حملة تشهير، أو مجرد رأي سياسي معارض، وذلك، انطلاقا من صحة الوقائع التي تسردها، وبناء على رأي المحكمة.

كذلك، لا بد من الاستجابة إلى طلب الحذف، في كل مرة تكشف البيانات المقصودة العرق، والمعتقد، والآراء السياسية، والميول الجنسية، أو غير ذلك، من بيانات حساسة. ومن بين المعايير أيضا، قدم المعلومة، والمدة الزمنية التي توضع فيها في متناول الجمهور، لاسيما متى تعلقت بقرار إدانة صادر عن محاكم الدرجة الأولى، تم إلغاؤه في الاستئناف.

ومن المفروض الاستجابة لطلب المحو، أيضاً، إذا ثبت تسبب المعلومات في ضرر لطالب المحو، أو في اثر سلبي غير متناسب، على حياته الخاصة؛ كان تكون المخالفة بسيطة، لكنها تؤثر على فرص الشخص المعني، بالحصول على فرصة عمل. كما يفترض محو كل البيانات، التي يمكن أن تؤذي الشخص، كرقم حسابه المصرفي، أو رقم جواز سفره، أو عنوان سكنه، أي كل معلومة، يمكن أن تساعد على الإيقاع به، أو الاستيلاء على هويته، أو على أمواله، على أن يراعى السياق، الذي نشرت فيه المعلومة. وهنا أيضاً، لا بد من مراعاة، ما إذا كان المحتوى المقصود، قد نشر بموافقة الشخص المعني، أو دون علمه. لكن في الحالتين، لا بد من احترام رغبة الشخص، في إزالة هذا المحتوى، والتوقف عن نشره.

ويرفض الطلب، في حال كان الهدف من نشر المعلومات والبيانات، إعلامياً. لكن ذلك، لا يعني سقوط حق الشخص المعني في طلب المحو، متى توافرت عناصر عدم دقة المعلومة، وقدمها، وعلاقتها بالحياة الخاصة، وتسببها بالأذى للشخص المعني، أو عندما يكون نشر المعلومة أو البيانات، تنفيذا لموجب قانوني؛ كحالة الأحكام، أو القرارات الإدارية، التي يفرض نشرها، لإعطائها مفعولا، أو لإعلانها. أما إذا كان الحكم جزائيا، فيختلف الأمر، إذا كان الجرم مشمولا بعفو عام، إذ يفترض قبول طلب المحو، على أن تدرس الهيئة المعنية، خطورة الجرم، والمدة التي مضت على تاريخ ارتكابه، في الحالات الأخرى.

ولقد أورد القانون التونسي، مادة خاصة بالحق في المحو، هي المادة 45، والتي نصت على: "إعدام المعطيات الشخصية"، مفندة الأسباب والحالات، والتي ترتبط مباشرة بانتهاء المدة المحددة لحفظها، أو بانتفاء الهدف من ذلك، مع استثناء المعطيات الشخصية، التي تكون قد أحيلت، أو معدة لتحال، إلى الأجهزة الأمنية، أو الهيئات الرسمية، المعددة في المادة 53، من القانون. ويلاحظ أن القانون التونسي، قد انتهج منهج القانون الفرنسي، في هذا المجال. أما المشترع الموريتاني، فقد خصص القسم الرابع لـ: "حق التصحيح والحذف"، أي انه أورده من ضمن الحقوق، التي اقرها لصاحب البيانات الشخصية.

وكان القانون القطري، قد نص على هذا الموجب في المادة 11، التي لحظت إجراءات، يفترض اتخاذها من قبل المسؤول عن المعالجة، لتلقي ودراسة الشكاوى، وطلبات الوصول إلى البيانات، وطلبات تصحيحها، أو حذفها. كما ورد موجب محو بيانات الأطفال، على المسؤول عن معالجة البيانات الشخصية، التي تجمع من مالك، أو مشغل أي موقع إلكتروني موجه للأطفال، بناء على طلب من ولي الأمر.

أما القانون المغربي، فقد نص على حق المحو، كما فعل المشترع المصري، في الفصل المخصص، لالتزامات المسؤول عن المعالجة، في اتخاذ الإجراءات الكفيلة، بإجابة طلبات التصحيح والمحو، المقدمة من أصحاب البيانات. وكذلك، بطريقة غير مباشرة، عبر إقراره عقوبات، على من يحتفظ بالبيانات الشخصية، لمدة أطول من تلك المحددة في التصريح، أو الترخيص، أو في القانون.

- **سرية المعلومات**

ترتبط سرية البيانات الشخصية، بتحفيز الاستقلال والكرامة الإنسانية. وفي غياب تعريف مجمع عليه، تعتبر السرية حق تحديد، متى، وكيف، وإلى أي مدى، يمكن

مشاركة المعلومات، التي تم الاطلاع عليها، (وهي هنا البيانات الشخصية) مع الآخرين. وبحسب هذا الموجب، المفروض لحماية البيانات الشخصية، لا يجوز للمسؤول عن المعالجة، السماح بالوصول إلى هذه البيانات، إلا للأشخاص المعنيين بمعالجتها، وللمدة الضرورية، لإنجاز الهدف الأساسي من جمعها.

فلا يجوز لفندق مثلا، الاستمرار بحفظ البيانات الشخصية، ورقم بطاقة الائتمان العائدة للزبون، بعد انتهاء مدة إقامة هذا الأخير لديه، وإتمامه موجب دفع المستحقات. بل يفترض بالفندق، أما محو البيانات، وأما تشفيرها، وأما اللجوء إلى تقنية إخفاء تحديد الهوية من خلالها، بحيث لا يعود تحديد الشخص المعني ممكنا، وعندها فقط، يسمح للفندق الاحتفاظ بها، لأغراض إحصائية، أو غيرها.

وقد شددت القوانين بمجملها، على سرية البيانات، سواء في معرض التطرق إلى الموجبات المترتبة على مسؤول المعالجة، ومنفذيها، أم في معرض ذكر المبادئ. وقد أكدت جميعها، على ضرورة إتلاف البيانات، تحقيقا لهذه الغاية، بعد الانتهاء من تحقيق هدف المعالجة، أو عندما يتوقف المسؤول عن المعالجة، نهائيا عن ممارسة أعمال المعالجة. كذلك نصت القوانين، على التزام كل من اطلع على البيانات، في معرض تنفيذ عمليات المعالجة، بعدم الكشف عنها، حتى بعد انتهاء فترة عمله عليها. وقد اعتبر معظم التشريع هذا الأمر، بمثابة الأسرار المهنية.

ويعتبر هذا الموجب، قريبا من موجب ضمان سلامة المعلومات، مع فرق اعتماده على التزام الأشخاص المأذون لهم بالاطلاع على البيانات الشخصية، لسبب قانوني أو إداري، بعدم الإفصاح عما يطلعون عليه من معلومات، بينما يرتبط أمن المعلومات، باعتماد تقنية تمنع هذا الاطلاع، على من لا يحق لهم أصلا، الاطلاع عليها.

- ضمان سلامة المعلومات

يعتبر ضمان سلامة المعلومات، مكملا لموجب سرية البيانات، من الناحية المادية، ومن الموجبات الأساسية، للمسؤول عن المعالجة. ويرتبط هذا الموجب، بضرورة الحفاظ على أمن المعلومات، ومنع تسريها، والحد من مخاطر انكشافها.

ويقتضي هذا الموجب، قيام المسؤول عن المعالجة، باتخاذ التدابير والإجراءات الضرورية لتحقيق ذلك، سواء أكانت تقنية، أم إدارية، أم تنظيمية، فيضع قواعد، وحدوداً، للاطلاع عليها، حتى للمعالجين، بحيث لا يسمح لهم بالوصول إليها، إلا في حدود ما هو ضروري، لتنفيذ مهام كل واحد منهم. كما يفترض استخدام برامج خاصة لمنع الاختراق، وكلمات سر لمنع الوصول إلى أي ملف، دون إذن.

ويشمل هذا الموجب، حماية المعلومات من أي تحوير، أو محو. فإذا أوكل أمر معالجتها، إلى جهات ثالثة، كان عليه تحديد موجبات كل طرف، في العقود المجراة لهذه الغاية، ولحظ التزامات تعاقدية، بحيث يضمن أمن البيانات. كما يجدر به، الإحاطة بالتهديدات الممكنة، نتيجة اختراق امن هذه البيانات، وبالمخاطر التي يمكن أن تحيط بأصحابها، في حال تعرضها للمحو، أو للتحوير، أو للانكشاف، بحيث يتمكن من حمايتها، بالشكل المناسب.

وقد سجل الاجتهاد الفرنسي، تشددا ملحوظا حيال هذا المبدأ، والموجب المنبثق عنه، والملقى على عاتق المسؤول عن المعالجة، حيث اعتبرت محكمة الدرجة الأولى، فرساي، أن تسرب عدد من الملفات إلى الصحافة، يبين أن المسؤول عن الملف، لم يتخذ جميع الإجراءات الضرورية، لمنع هذا التسرب، ما يوجب إعلان مسؤوليته[144].

[144] En 2002, le TGI de Versailles a condamné le responsable du traitement des données d'une entreprise car il avait constitué un fichier de gestion du personnel dont une partie avait été transmise à la presse. La cour a dit: «il appartenait à X qui dirigeait la constitution du fichier d'assurer la totale confidentialité des opérations. La fuite des 38 documents communiqués à la presse montre qu'il n'a pas pris toute les précautions utiles, il sera donc déclaré coupable de ces faits.»
https://www.kilianver.net/?page_id=816

وكانت الهيئة الوطنية للحريات والمعلومات، قد أصدرت قرارا، بتغريم شركة فرنسية، مبلغ مئتين وخمسين ألف يورو، نتيجة عدم اتخاذ المسؤول عن معالجة البيانات، جميع الإجراءات الضرورية، والمناسبة لطبيعة البيانات والمخاطر التي تهددها، لحماية سلامتها، ومنع تحويرها، أو تضررها، والوصول إليها، من قبل أشخاص ثالثين، غير مسموح لهم بذلك[145].

وغني عن القول، أن أخذ النتيجة بعين الاعتبار، لتقرير كفاية الإجراءات وملاءمتها، يعني تحويل هذا الموجب، إلى موجب نتيجة، يفرض على المعني به، ضمان تنفيذ ما التزم به، وبالتالي، يكفي عدم الحصول على النتيجة المرجوة لإثبات الخطأ، بينما من المفترض بالمدعي، في حالة موجب الوسيلة، أن يثبت خطأ المدعى عليه، أو إهماله، أو عدم انتباهه، ما يجعل الإثبات، اكثر صعوبة.

في هذا الإطار، تميز التشريع الإماراتي، بإلزامه المؤسسات في القطاعين العام والخاص، بتصنيف البيانات، كجزء من الإجراءات التقنية، الخاصة بأمن البيانات وحمايتها. فنصت المادة الحادية عشرة منه، على التزام الإدارات الحكومية الرسمية، بتصنيف بياناتها، وفقا للدليل الوطني، الذي يعرف ب "دليل دبي"، وبوضع خطة زمنية، لنشر وتبادل البيانات المتوفرة لديها، أو تحديد المعوقات التي تمنعها من ذلك، ليتم بعد ذلك، رفعها إلى مؤسسة بيانات دبي لاعتمادها.

كما فرض على الإدارات المختلفة، تزويد المؤسسة بأية معلومات، أو تقارير تطلبها، بشأن نشر وتبادل البيانات، والسياسات والإجراءات والأدلة والضوابط والاشتراطات المعتمدة من المؤسسة.

---

[145] - Commission Nationale de l'Informatique et des Libertés Délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données L'article 34 de la loi du 6 janvier 1978 modifiée dispose que le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès
https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037013610&fastReqId=1003469497&fastPos=1

أما مزودو البيانات في القطاع الخاص، فيفترض بهم بحسب المادة الثانية عشرة، الالتزام بكافة السياسات، والآليات، والأدلة، والشروط، التي تحددها مؤسسة بيانات دبي، في مجال نشر وتبادل البيانات.

وكانت المادة السابعة، قد فرضت تصنيف بيانات دبي، وفقا للمعايير المعتمدة، فيما خص البيانات المفتوحة، والبيانات المشتركة، وذلك، وفقاً لدليل بيانات دبي، الذي تعتمده مؤسسة بيانات دبي، بالتنسيق مع مركز دبي للأمن الإلكتروني.

هذا، وتتوزع البيانات وفقا للتصنيف المذكور، بين بيانات مفتوحة، يمكن لأي كان الحصول عليها، وبيانات مشاركة، تملكها الهيئات المختلفة وتضعها بتصرف الهيئات الأخرى، سواء لتستخدمها، أو لتعيد استخدامها، والمعلومات الخاصة، Confidential، التي يتم تبادلها بين الهيئات، وفق معايير المسؤولية المهنية، والبيانات الحساسة، والتي يتم تبادلها بين مجموعات حصرية، وفقا لرقابة مشددة، والبيانات السرية، التي يتم تبادلها بين عدد من الأفراد، برقابة مشددة، أيضا.

وذكرت المادة 9، أنه على مزودي البيانات، توفير بيانات دبي الموجودة لديهم، أو التي يتم استحداثها أو تطويرها من قبلهم، وفقاً للسياسات التي تعتمدها مؤسسة بيانات دبي في هذا الشأن، ويجب عليهم، على وجه الخصوص، الالتزام بما يلي: نشر البيانات المفتوحة الخاصة بهم، وفقاً للضوابط والقواعد المعتمدة لدى المؤسسة، وتبادل البيانات المشتركة الخاصة بهم، وفقاً للضوابط والشروط المعتمدة لدى المؤسسة، وذلك، إضافة إلى عدم المساس بقواعد سرية البيانات، أو بحقوق الملكية الفكرية، وأن تكون البيانات المنتجة أو المعالجة من قبلهم، قابلة للقراءة وبأشكال فنية متعددة، والامتثال للقواعد التنظيمية والبروتوكولات الفنيّة المعتمدة من قبل المؤسسة، بشأن نشر وتبادل البيانات.

- **الشفافية**

لا يوجد تعريف موحد يمكن اعتماده لهذا المصطلح، إلا أن تحديده ممكن، من خلال ما يؤشر إليه عادة؛ أي الحق في الاستعلام، والحق في الوصول إلى المعلومات. وبشكل عام، تتعلق الشفافية، بإمكانية الوصول إلى معلومات محفوظة، ضمن دائرة خاصة، ودقة، وصحة المعلومات، وبما يمكن للمواطن القيام به، في حال كان من يحتفظ بالمعلومات، لا يوفر الوصول إليها، بشكل كاف.

وغالبا، يستخدم مصطلح الشفافية، لوصف الممارسات، الاجتماعية، أو الاقتصادية، أو الإدارية، التي تسترشد بالإخلاص، في أداء مهمات ووظائف معينة، وبإمكانية الوصول الكامل إلى المعلومات، في المجالات، التي تهم الرأي العام. ويرتكز هذا المصطلح، إلى الحرص، على إرساء قواعد المسؤولية عن نشاط ما، ورصد الأخطاء، والإقرار بها، في مجالات، يمكن أن تمس بحقوق الآخرين.

وتعتبر الشفافية، أحد أهم العناصر المؤسسة للأمن القانوني، واستقرار التعاملات في المجتمع. بينما يعتبر غيابها، أحد أهم العوائق، أمام الوصول إلى العدالة، وتطبيق القانون، بشكل صحيح. فعندما يجهل المواطن قواعد اللعبة؛ وهي هنا، حقوقه، وكيفية ممارستها، تنعدم الفائدة من القانون، بشكل عام، ومن قوانين حماية البيانات الشخصية، بشكل خاص.

وهكذا، يرتبط هذا المبدأ، بموجب المسؤول عن معالجة البيانات الشخصية في إعلام صاحبها، عن رغبته في جمعها، ومعالجتها، وعن الأهداف، والاستخدامات المحتملة، والجهات التي ستنتقل إليها، من جهة أولى، ومبدأ التبليغ، أو التصريح إلى السلطة الوطنية المسؤولة عن حماية البيانات، من جهة ثانية.

ويعتبر مبدأ الشفافية، في كافة المجالات، لاسيما الحوكمة، الأساس الذي يؤمن الثقة، في إمكانية ممارسة الحقوق الأخرى، التي يقرها القانون لصاحب البيانات.

إذ لا يمكن الرجوع إلى بيانات، أو تصحيحها، أو الاعتراض على معالجتها، وطلب تعديلها، ومحوها، إلا متى كان الشخص المعني، عالما بهذه المعالجة.

- **احترام حقوق أصحاب البيانات**

يهدف إقرار حقوق أصحاب البيانات، إلى إعطاء الأشخاص المعنيين، إمكانية السيطرة على بياناتهم. لذا، يتعين على المسؤول عن المعالجة، تمكينهم من ممارسة هذه الحقوق، سواء عبر إعلامهم بها، أو عبر مساعدتهم على معرفة الجهة التي يفترض مراجعتها بهذا الشأن، أو عبر اطلاعهم على الطريقة التي يجب اتباعها لذلك.

وفي حال ممارسة أصحاب البيانات لحقوقهم، يفترض الالتزام بالاستجابة لمطالبهم، خلال مهلة معينة. ويعتبر هذا الأمر، تجسيدا للحق في الاستعلام، الذي يفرض إعلان هوية المسؤول عن المعالجة، والهدف منها، والصفة الجبرية، أو الاختيارية، للأسئلة المطروحة خلال عملية جمع المعلومات، والجهات التي ستنتقل إليها، والحقوق التي يتمتع بها صاحب البيانات (الوصول إلى المعلومات، والتعديل، والاعتراض).

- **إعلام أصحاب البيانات (الأشخاص المعنيون)**

يعتبر حق الشخص، في أن يعرف بما يجمع من معلوماته، واحدا من أساسيات الحماية، لاسيما وان الأسباب الحقيقية للتشريع، هي في منع عملية جمع البيانات الشخصية، ومعالجتها، دون علم أصحابها. ولقد أوردنا سابقا، حقيقة عدم اقتصار هذه الممارسة، على الأجهزة الأمنية الحكومية، وامتدادها إلى الشركات في القطاع الخاص، الأمر الذي يوسع دائرة التهديدات، ويرفع مستوى التحديات التشريعية والتقنية.

وفي هذا السياق، تبدو واضحة، ضرورة إلزام المسؤول عن المعالجة، باتخاذ جميع الإجراءات والتدابير الضرورية، لتوفير المعلومات اللازمة، لأصحاب المعلومات الشخصية، بطريقة دقيقة وواضحة، مفهومة، شفافة، وسهلة الاستيعاب.

ويكون هذا صحيحا، عند استخدام تعابير سهلة وواضحة، لا تثير الشك، ولا تحتمل التأويل، لاسيما متى كان صاحب البيانات من فئة الأطفال، الأمر الذي شددت عليه جميع القوانين. ولهذا الغرض، يمكن أن تكون المعلومات مكتوبة، أو شفهية، كما يمكن أن تكون رقمية.

ويفترض بالمسؤول عن المعالجة، الإجابة عن أي سؤال، يمكن أن يطرحه صاحب البيانات، حول عملية المعالجة، وأهدافها، والجهات الثالثة التي يمكن أن تنقل إليها، وذلك ضمن مهلة زمنية معقولة، يمكن أن تقصر أو تطول، نسبة إلى طبيعة، وحجم نشاط الجهة المسؤولة عن المعالجة.

في الواقع، يترجم الالتزام بهذا المبدأ، من قبل المسؤول عن معالجة البيانات، أو من قبل المتعاقد من الباطن، عبر اعتماد الموقع، أو مقدم الخدمات، لما يسمى بـ"سياسة الخصوصية". وتحوي هذه الأخيرة، جميع المعلومات التي توضح: فئة البيانات الشخصية التي تجمع، الهدف من جمعها، كيفية استخدامها، مدة الاحتفاظ بها، الجهات الثالثة التي يمكن أن تطلع عليها، كيفية حمايتها، التقنيات المستخدمة في جمع البيانات، وكيف يمكن للشخص المعني، أن يسيطر على كل مرحلة من هذه المراحل.

في هذا السياق، لابد لسياسة الخصوصية، التي يعتمدها الموقع، أن تحدد الجهة المسؤولة عن المعالجة، والجهة المعالجة، وان تعلم الشخص المعني بحقوقه، في رفض السماح بمعالجة بياناته، والوصول إلى المعلومات التي تجمع عنه، والاعتراض، وطلب التعديل، والتيويم، والمحو.

موجبات المسؤول عن المعالجة، والمعالج، والمتعاقدين معهما

فرضت القواعد الجديدة عددا من الموجبات، على المسؤول عن المعالجة، والمعالج، والجهات الثالثة، التي تتعاقد معهما، لتنفيذ عمليات إدارة، أو تحليل، أو محاسبة، أو أي نشاط آخر، يشمل العمل على البيانات الشخصية، مدخلة بذلك مفهوم المسؤولية المشتركة، والذي يمكن أن ينظم من خلال العقود، التي يبرمها المراقب أو المعالج، لتنفيذ المهمات المختلفة. بالإضافة إلى ذلك، أرست هذه القواعد، مبدأ المساءلة، والذي يفرض على الشركات المعنية، احترام الموجبات التي تنص عليها، من جهة أولى، واثبات اتخاذها للإجراءات التقنية والتنظيمية المناسبة، التي تضمن هذا الاحترام، من جهة ثانية.

وكانت القواعد الأوروبية الجديدة، قد فرضت عددا من الموجبات، التي تختلف حسب دور الشركة، كمراقب أو كمعالج للبيانات، علما أن الشركة يمكن أن تقوم بالدورين معا، وتكون مسؤولة في هذه الحال، عن الالتزام بالموجبات مجتمعة، حيث يعتبر المراقب صاحب القرار في المعالجة، وتحديد أهدافها، بينما يعتبر المعالج، منفذا لأوامره.

وتتوزع موجبات المسؤول عن المعالجة، كما المعالج، على ما هو ذي طبيعة إدارية، تقنية، إجرائية، وقانونية. ويمكن تلخيص أهمها بالالتزام:

- بمعالجة البيانات حسب منطوق القواعد الجديدة[146]، على أن تكون هذه البيانات صحيحة، دقيقة، متناسبة، ومحددة بالهدف من معالجتها، وعلى أن تكون جميع عمليات المعالجة موثقة، وممسوكة في سجلات معدة لهذه الغاية.
- التأكد، في حال عمله مع معالج للمعلومات، أو أي متعاقد آخر، من احترام أحكام القواعد، على أن يدون هذا الأمر، في العقد الذي يوقع بينهما.

[146] - (article 6 (1)).

- اتخاذ الإجراءات المناسبة لحماية أمن هذه البيانات، ومنع تعرضها للتلف، أو للتعديل، أو للتسرب، أو للاختراق، أو الضياع عن طريق الخطأ، عرضا أو قصدا، وذلك عبر احترام مبدأي: "الحماية من خلال التصميم"، و"الحماية المعدة سلفا[147]"؛ ما يعني ضرورة اتخاذ إجراءات الأمن، بدءا من مرحلة التحضير للمعالجة، مرورا بمرحلة المعالجة، وصولا إلى مرحلة عرض الخدمات أو المنتجات.
- الحرص على إجراء تقييم لنظام المعالجة[148]، الذي يعتمد عليه، ولتأثيره على حقوق وحريات، الأشخاص الطبيعيين، إضافة إلى ضرورة احترام قواعد تبادل البيانات، عبر الحدود، والتي توجب ذلك مع جهات خاضعة لدولة، تؤمن حماية مناسبة لها، أو بموجب عقد، أو تنظيم داخلي، بين الجهة التي تتولى نقلها، والجهة التي تتلقاها.
- إعلام صاحب البيانات، بعملية المعالجة، ولو لم يكن هذا المراقب، هو من تلقاها، مباشرة، كحالة شرائه للبيانات من جهة ما، وهذا، كما هو معلوم، شديد الرواج، مع توسع حركة الاتجار بلوائح البيانات الشخصية. كما أضيف موجب الإبلاغ عن أي اختراق[149]، أو تسرب للمعلومات، دون إبطاء، وخلال 72 ساعة، على أبعد تقدير، من تاريخ العلم به، إلى السلطات المختصة بحماية البيانات الشخصية، وإلى الأفراد انفسهم، في حال وجود خطر، يمكن أن يهدد حرياتهم، وحقوقهم.

وفي حال التأخر عن الإبلاغ، خلال المهلة المحددة، على المراقب أن يبرر هذا التأخير. كما يفترض بالمعالج، أن يبلغ المراقب، بأي تسرب أو اختراق، خلال المهلة المحددة نفسها. ويفترض بالإعلام، أن يحتوي على فئات أصحاب البيانات، التي تم اختراقها، والعدد التقريبي للأفراد الذين تسربت بياناتهم، كما فئات الملفات

[147] - by default

[148] - Data Protection Impact Assessment (DPIA)

[149] - Art. 33 GDPR Notification of a personal data breach to the supervisory authority

وعددها، إضافة إلى تحديد اسم المسؤول عن حماية البيانات لدى الشركة، والذي يمكن الاتصال به، للحصول على المزيد من المعلومات.

كذلك، لا بد من تحديد الإجراءات، التي سيتم اتخاذها، لمعالجة الاختراق، والحد من نتائجه السلبية، وتأثيره على الأشخاص المعنيين، على أن يتم توثيق هذه التفاصيل، والاحتفاظ بها، لمساعدة السلطة المختصة، في الاطلاع عليها، وتقييم مدى التزام الشركة المعنية، بالقواعد الأوروبية لحماية البيانات. كما تلتزم الشركات، بتقديم تقرير حول البيانات، في غضون 30 يوما، إذا طلب منها ذلك، ما يوسع نطاق المساءلة عن حمايتها.

مما لا شك فيه، أن هذه الموجبات، تؤسس لحماية فاعلة للبيانات ذات الطابع الشخصي، ويبقى أن الموجب الأكثر ارتباطا بممارسة الحق في المحو، الذي أقرته القواعد الجديدة، هو الموجب الملقى على عاتق مراقب البيانات، بإعلام الجهات الثالثة، بطلب المحو، الذي يقدم إليه، من صاحب العلاقة.

ويعتبر هذا الموجب، الذي أقرته المادة 17، موجب نتيجة، لاسيما لجهة ضرورة إبلاغ الجهات الثالثة، التي أعطيت الحق بنشر البيانات والمعلومات، بان صاحبها يطلب حذفها. ويبدو واضحا، أن هذا الموجب، هو رهن بمسؤولية مراقب المعلومات، عن الأشخاص الثالثين، الذين تولوا عملية النشر، اي في كل مرة يكون هو من أعطاهم الإذن بنشرها.

- **المفاهيم الجديدة**

في هذا السياق، لا بد لنا أن نتوقف عند المفاهيم الجديدة، التي أقرتها القواعد الأوروبية الجديدة، والتي أخذت مما هو معمول به، في النظام القانوني الأميركي، والتي أسست لهذه الموجبات، أي المساءلة، ودراسة الأثر على الخصوصية، والخصوصية منذ التصميم.

» المساءلة

يرتبط هذا المفهوم بآليات الحوكمة الرشيدة، وإمكانات محاسبة المسؤول عن تنفيذ مهمة ما. ولا يعتبر هذا المفهوم جديدا، في مجال حماية البيانات، لكن المادة الرابعة والعشرين، من القواعد الأوروبية الجديدة، قد نصت عليه صراحة، في المادة الخامسة[150]، كواحد من مبادئ معالجة البيانات، لتعطي تفاصيل حول كيفية الالتزام به في المادة [151]24. وقد نصت هذه المادة الأخيرة، على موجب اتخاذ "التدابير التقنية والتنظيمية المناسبة"، لكي تتمكن المؤسسة المعنية بمعالجة البيانات، من "إثبات" امتثالها لأحكام القانون. ويشمل ذلك، "تنفيذ سياسات حماية البيانات المناسبة"، ومراجعتها، وتحديثها، عند الضرورة.

وتعتمد التدابير التي يجب أن تلجأ إليها المنظمة، لإثبات الامتثال، على طبيعتها، وحجمها، وهيكلتها، وعملية معالجة البيانات التي تقوم بها. لذلك، قد تختلف آليات الامتثال، لكن المدلول الأهم، لمبدأ المساءلة، هو مطالبة الشركات بتحمل المسؤولية الكاملة، عن حماية بياناتها، طوال دورة حياة البيانات التي تعالجها.

أما الترجمة العملية لتطبيق هذا المبدأ، فهي أولا في اعتماد مقاربة استباقية، ومنهجية، بحيث تؤخذ حماية البيانات كالمحور الأساس، منذ بداية عمليات المعالجة، إلى حين انتهائها. ولذلك، يفترض اتباع الخطوات الآتية، على سبيل المثال:

- الاحتفاظ بسجلات خاصة، تدون فيها جميع المعلومات اللازمة، لمتابعة

[150] - Article 5 - Principles relating to processing of personal data
Personal data shall be: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

[151] - Article 24 - Responsibility of the controller
Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

عملية المعالجة، بحيث تشمل أغراضها، وطبيعة البيانات، وفئات الأشخاص الطبيعيين، ومواضيع البيانات، وعمليات نقلها إلى الخارج، والجداول الزمنية لحفظها ومحوها، وتدابير الحماية؛ الفنية، والتنظيمية، المطبقة على أنشطة المعالجة.

- ضمان الاتصال الفاعل والشفاف، مع أصحاب البيانات، حول تفاصيل معالجة بياناتهم الشخصية، وحقوقهم.
- مراجعة شاملة، لطرق الاشتراك، وسياسات الخصوصية، وأية مصطلحات أخرى، خاصة بحماية البيانات، على الموقع.
- مراجعة الطريقة، التي يتم بها جمع موافقات الأشخاص المعنيين بالبيانات، للتأكد من أنها واضحة، ودقيقة، وضامنة لحرية الموافقة.

وهكذا، يلقى مبدأ المساءلة، اهتمامًا متجددًا، لأن القواعد الأوروبية باتت تفرضه كالتزام قانوني، يساعد المؤسسات المعنية، على تنظيم نفسها، وتحديد القواعد، التي تراها الأنسب لها، ولطبيعة عملها، والتي يمكن اعتمادها، كأساس لمحاسبتها، وقياس مدى التزامها بقوانين الحماية.

» تقييم الأثر على الخصوصية Privacy Impact Assessments

يتعلق هذا الأمر، بواجبات المسؤول عن المعالجة، في إجراء تقييم للأثر، الذي يمكن أن تتركه المعالجة على البيانات الشخصية، وتوثيقه، قبل البدء في المعالجة المخطط لها. ويصبح هذا الأمر ضروريا، عندما تتوافر احتمالات، وجود مخاطر عالية[152]، على حقوق وحريات الأشخاص الطبيعيين، نتيجة للمعالجة. بالإضافة إلى ذلك، يجب القيام بهذا التقييم، إذا توافر واحد من الأمثلة، التي نصت عليها المادة

[152] - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679
"The carrying out of a DPIA is only mandatory where a processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced"

35 فقرة 3[153]، من القواعد الأوروبية. ومن المفترض، أن تحدد سلطة الرقابة على تنفيذ القانون الخاص بحماية البيانات، أساسيات القيام بهذا التقييم. بالالتزام الأساسي للتنفيذ.

وكانت مجموعة الـG29، قد وضعت عددا من المعايير، التي تشكل مؤشرًا لخطر كبير، على حقوق، وحريات الشخص الطبيعي، مثل التسجيل/التنميط، والقرارات التي تؤخذ أوتوماتيكيا، والتي يمكنها، أن تؤدي إلى عواقب قانونية.

يضاف إلى ذلك، معالجة بعض أنواع البيانات الشخصية الخاصة؛ كالتي تتم معالجتها على نطاق واسع، أو بيانات الأشخاص العاجزين، أو ذوي القدرة المحدودة على التصرف، أو لدى استخدام تقنيات جديدة، أو نقل البيانات إلى بلدان، خارج الاتحاد الأوروبي، وأية معالجة يمكن أن تعيق ممارسة الأشخاص لحقوقهم.

أما عملية التقييم، فلا بد وأن تتم، انطلاقا من ضرورة احترام، الحقوق الأساسية للإنسان، من جهة أولى، وفكرة إدارة المخاطر، التي تساعد على اتخاذ التدابير التقنية، والإدارية، والقانونية الضرورية، لحماية البيانات الشخصية، من جهة ثانية.

وكانت الهيئة الوطنية الفرنسية للمعلوماتية والحريات، قد حددت مراحل اربع، للتقييم، هي: دراسة سياق عملية المعالجة، والتدابير المتخذة، أو المفترض اتخاذها، والمخاطر؛ لاسيما منها ما يمكن أن يعرض الخصوصية للخطر، وصولا إلى المرحلة الرابعة، إلا وهي تقييم صحة المنهجية المتبعة، أو التي ستتبع لاحترام الالتزامات القانونية، ومعالجة المخاطر.

[153] - Article 35 – Data protection impact assessment Where The controller
A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
a systematic monitoring of a publicly accessible area on a large scale.

وغني عن القول، أن احترام هذه المراحل، لا بد وأن يؤدي عمليا، إلى توثيق عملية التقييم هذه.

» الخصوصية حسب التصميم **Privacy by design**

يمكن اختصار هذا المفهوم، بأنه إجراء تقني يلقي الضوء، على أهمية الهندسة المعلوماتية، في حماية البيانات الشخصية، من خلال الاعتماد على بناء البرامج، والتطبيقات، بطريقة تأخذ حماية الخصوصية بعين الاعتبار، منذ البداية. والأمثلة التي يمكن سوقها هنا كثيرة، نذكر منها، تقنيات التصفح بهوية مجهولة[154]، والتي تسمح بمحو جميع آثار المتصفح على الإنترنت، كما وبإتلاف الكعكات، التي استخدمت، فور انتهاء، عملية تصفح المواقع.

ونذكر أيضا، التقنيات الخاصة بتحسين الخصوصية[155]، والتي تسمح بفك الارتباط، بين البيانات الشخصية، وبيانات الاتصال، بحيث تسمح بتوفير خدمة خاصة بالمتصفح، دون أن تؤدي بالضرورة، إلى تحديد هويته.

وكانت المادة الخامسة والعشرون[156]، من القواعد الأوروبية الجديدة، قد نصت على هذا المبدأ، فألزمت المسؤول عن المعالجة، اتخاذ التدابير المناسبة، قبل بدء عملية المعالجة، وخلالها، لضمان الحفاظ على خصوصية الأشخاص المعنيين، سواء من خلال استخدام أسماء مستعارة، أو تصغير حجم البيانات، أو اتخاذ التدابير التنظيمية والإدارية، التي تمنع الوصول إلى البيانات الشخصية، دون مسوغ شرعي.

[154] - Anonymous surfing

[155] - Privacy enhancing Technologies(PETs)

[156] - Art. 25 GDPR Data protection by design and by default Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
1 The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. An approved certification mechanism

في حقوق أصحاب البيانات

كما يجهل العديد من المبحرين على الإنترنت، حجم ما يجمع عنهم من معلومات، وما يعالج من بياناتهم الشخصية، أو الأهداف الكامنة وراء هذه المعالجة، هكذا لا يدرك البعض منهم، أن لديه إمكانية استعادة زمام السيطرة، على حدود ما يكشف عن حياته الخاصة، والأمور التي تتعلق بشخصه، وشخصيته، من خلال الحقوق التي تمنحه إياها، قوانين حماية البيانات الشخصية.

فقد لحظت جميع قوانين الحماية، دون استثناء، أحكاما تقر فيها، بعدد من الحقوق لأصحاب البيانات الشخصية، تتوزع بين الحق في معرفة أغراض المعالجة، بطريقة لا لبس فيها، وحق الاطلاع على البيانات، وممارسة الحق في الموافقة على المعالجة أو رفضها، وحق الاعتراض عليها، وطلب وقفها، والرقابة على دقة البيانات، وصحتها، وطلب محوها، وتعديلها.

- **الموافقة على جمع البيانات**

بصورة عامة، تسمح جميع القوانين المعمول بها، في مجال حماية الخصوصية، وسرية المعلومات، بعملية جمع البيانات، واستخدامها، ضمن حدود معينة، ترتكز بشكل أساسي، على مدى موافقة صاحبها. ويمكن لهذا الأمر، أن يجعل الصورة مقبولة، إذ يعطي انطباعا، بنوع من السيطرة للشخص المعني، على بياناته. لكن الواقع، بعيد تماما عن ذلك. فمستخدم الإنترنت، نادرا ما يقرأ الشروط الطويلة، والبنود الغامضة، التي تعرض عليه للموافقة عليها، قبل إعطائه حق استخدام برنامج، أو تطبيق، أو منصة إلكترونية، ما يعني أن الموافقة التي يعطيها، ليست صادرة عن إرادة صحيحة.

في الواقع، ومن خلال الممارسات، التي كانت معتمدة حتى اليوم، يمكن إثبات حصول الموافقة، بعدد من الطرق، سواء عبر التعبير الكتابي، أو القيام بعمل

معين، وذلك بحسب الظروف. فبعض مزودي وموردي الخدمات، يطلبون من المستخدم الضغط على زر "أنا موافق"، ليعبر عن موافقته على عدد من الشروط والأحكام، بينما يعبر البعض الآخر، مجرد استخدام الموقع، أو التطبيق، بمثابة الموافقة، على أحكام وشروط خفية، منصوص عليها، في مكان ما من الموقع. ويمكن لجميع هذه الوسائل أن تخلق علاقة قانونية ملزمة، هي ما يعرف ب "العقد"، بحسب اللغة القانونية، بالرغم من كونها ممارسات غير سليمة.

فالمستخدم في البيئة الرقمية، الذي يغرقه كم هائل من المعلومات، ليس مجبرا على البحث، والتنقيب، لإيجاد هذه الأحكام والشروط، أو للاطلاع على سياسة الخصوصية. فمعظم مستخدمي الإنترنت، لا يقرؤون أحكام وشروط الاستخدام، التي تظهر على الشاشة. وغالبا ما لا يتمكنون من فهم نوعية البيانات الشخصية التي يطلب منهم الموافقة على الإفصاح عنها، ومعالجتها، كما لا تتوفر لهم إمكانات الإحاطة، بتفاصيل المعالجة، وتأثيرها عليهم، سواء عندما يوافقون على شروط استخدام الموقع، أو البرنامج، أو التطبيق، أو عندما يضغطون، على زر الموافقة.

والأدهى، أن جميع مستخدمي الإنترنت تقريبا، لا يمكنهم أن يتوقعوا ما تتيحه التقنيات الحديثة، وقدرات الذكاء الاصطناعي، من آفاق، وإمكانات مختلفة، ومعقدة أحياناً كثيرة، على مستوى معالجة البيانات الشخصية. وإذا تركنا جانبا، تعقيدات وفذلكات العقود، التي تعرض عليهم، حيث ترد جميع التفاصيل، والمعلومات، حول كيفية معالجة البيانات واستخداماتها، فان هذه العقود لا تعدو كونها، عقود إذعان، لا يملك المستخدم خيار رفضها، إلا إذا قرر التخلي عن استخدام الموقع أو الخدمة.

تنص القوانين، بشكل عام، على تعريف العقود وعناصرها، وشروط صحتها. فتعتبر انه في العقد بين شخصين، هنالك عرض من طرف أول، وقبول من طرف آخر،

أو عدة أطراف، مع توافر نية خلق التزام قانوني، ومقابل للموجبات، وأهلية قانونية للدخول في التزام عقدي، وإرادة حرة وصحيحة، وفهم وموافقة لموضوع الالتزام. وهكذا، تتأثر صحة العقد، بأي شكل من أشكال الضغط الذي يعيب الإرادة، أو التصريح الكاذب، أو التأثير غير المسوغ، أو الموافقة غير الواعية.

وبناء عليه، فأية موافقة بالضغط على زر "أنا موافق"، أو الاتفاق على اتفاقية المتصفح، أو البرنامج، أو التطبيق، تنقصها النية الواضحة لخلق التزام قانوني، كما ينقصها فهم واستيعاب كامل، وموافقة صريحة. علاوة على ذلك، يمكن أن تعاني الإرادة في هذه الحالة، من الإكراه، والتأثير غير المبرر، والاتفاق غير المقبول، عندما لا يستطيع المستخدم، مناقشة أو تعديل، شروط وأحكام الاستخدام.

ويصبح الأمر أشد تعقيدا، عندما يتعلق بالأجهزة الذكية، حيث تطلب موافقة الشخص المعني، لاستخدام عدد من التطبيقات، وبطرق تقنية غير واضحة، كتبادل البيانات بين تطبيقين مختلفين، أو سحب لائحة الأصدقاء، وعناوينهم. وان كنا لن نتوقف عند هذا الأمر الأخير للتعمق فيه، إلا انه تجدر الإشارة، إلى تحول الشخص المعني، إلى مصدر لجمع بيانات شخصية، لا تخصه، وإنما تخص أهله وأصدقاءه، ومعارفه، وربما زبائنه.

وكانت القواعد الأوروبية الجديدة، قد أضافت الحق في الرجوع عن الموافقة، في أي وقت يراه صاحب البيانات.

كما تشددت هذه القواعد، في أصول الحصول على موافقة صاحب البيانات بجمعها، ومعالجتها، ونقلها، عبر اشتراط موافقة صريحة، غير ضمنية، تفترض معرفة بأهداف العملية، وبالحقوق المرتبطة بها. وتجدر الإشارة هنا، إلى أن القوانين العربية، قد أقرت هذا النوع من الموافقة، الصريحة، والواضحة.

وقد تشابهت هذه القوانين، لناحية إقرار مضمون هذه الحقوق، وان اختلفت لناحية التعبير عنها. فقد نظمها المشترع التونسي، في القسم الثالث، من القانون، المعنون: "في حقوق المعني"، تحت الحق في الموافقة، والحق في النفاذ، وحق الاعتراض، علما أن هذا القانون، اقر حق الاستعلام، وحق التصحيح، وطلب المحو، أو التيويم، ضمنا من خلال "حق النفاذ".

فقد نصت المادة الـ32، على أن المقصود بحق النفاذ، هو حق الشخص المعني، في الاطلاع على جميع المعطيات الشخصية الخاصة به، وطلب إصلاحها، أو إتمامها، أو تعديلها، أو تحيينها. ويشمل الحق في النفاذ، أيضا، الحق في الحصول على نسخة عن البيانات. وكان المشترع الموريتاني، قد اعتمد نصا مشابها.

وخصص التشريعان المصري والمغربي الباب الثاني، لسرد هذه الحقوق، على الشكل الآتي: الحق في الأخبار أثناء تجميع البيانات، الحق في الولوج أو الوصول، الحق في التصحيح، الحق في الاعتراض، منع الاستقراء المباشر، انعدام الآثار؛ بمعنى عدم جواز الحكم على شخص معين، وتقييم شخصيته، وسلوكه، بناء على معلومات أخذت بنتيجة عملية معالجة البيانات إلكترونيا. ما يعني حماية الأشخاص الطبيعيين، من نتائج القرارات، التي يمكن أن تتخذ آليا، نتيجة تحليل بياناتهم الشخصية، والمعلومات المتوافرة عنهم.

أما التشريع القطري، فقد خصص، هو الآخر، الفصل الثاني، لتعداد حقوق الأفراد، بشكل مقتضب، إلا انه قرن حق الحصول على نسخة من البيانات الشخصية، بموجب دفع بدل "لا يجاوز مقابل الخدمة". وقد ربط هذا التشريع، أمر تنظيم حق الوصول إلى البيانات، ومراجعتها، وإخطار الشخص المعني، بأي إفشاء لبياناته الشخصية، إضافة إلى حصوله على نسخة منها، بقرار يصدر عن الوزير المختص، يحدد ضوابط العملية، وإجراءات ممارسة هذه الحقوق.

- **حق الاعتراض**

يمكن لصاحب البيانات، الاعتراض على معالجة بياناته الشخصية، لأسباب مشروعة. كما يمكنه رفض استخدام هذه البيانات، في دراسات وأبحاث تجارية؛ وذلك دون أن يكون مجبرا على تقديم اي تبرير، أو سبب. كما يمكنه ممارسة هذا الحق، سواء في مرحلة جمع البيانات، أو في مرحلة لاحقة. فلكل شخص من حيث المبدأ، حق تقرير طريقة استخدام بياناته، بحيث يرفض إدراجها ضمن ملفات إلكترونية معينة، أو نقلها إلى جهات ثالثة.

وتتم ممارسة هذا الحق، أيضاً من خلال رفض الإجابة على الأسئلة التي تطرح عليه حول بياناته الشخصية، خلال عملية الجمع، متى كانت هذه الأخيرة غير ملزمة، ورفض إعطائه الموافقة الخطية، التي تعتبر إلزامية، في معالجة البيانات الحساسة، كالانتماء الديني، أو الميول الجنسية، أو السياسية. كذلك، يمكنه ممارسة هذا الحق لطلب محو بياناته، من الملفات ذات الأهداف التجارية. أما على الأنترنت، فيمكنه ببساطة أن ينتقي الرفض، في خانة الاختيار بين الرفض والموافقة، والتي ترد، على نموذج جمع المعلومات.

أما الرفض في مرحلة لاحقة، فيتم من خلال الاتصال، بالمسؤول عن المعالجة، أو إرسال بريد إلكتروني، أو غير ذلك، دون تكبده أية كلفة، وعلى المسؤول الإجابة، خلال مهلة يحددها القانون. ولا يمكنه الاحتجاج بعدم وضوح الطلب، أو بأي عذر آخر؛ إذ يفترض به الرجوع إلى مقدم الطلب، وطلب استيضاحات، أو أية معلومة ضرورية، لبناء الاستجابة عليها. وفي حال قرر المسؤول عن المعالجة رفض الطلب، فعليه موجب تقديم التبريرات اللازمة، لجعل رفضه قانونيا، وإلا يمكن لمقدم الطلب، مراجعة الجهة المعنية؛ وهي في هذه الحالة، الهيئات أو الأجهزة المسؤولة، عن حماية البيانات الشخصية.

- حق التصحيح

يحق لكل شخص أن يطلب تصحيح بياناته الشخصية، أو استكمالها، أو تيويمها، أو حجبها، أو محوها، متى كانت هذه البيانات غير صحيحة، أو غير كاملة، أو غير مناسبة، أو قديمة، أو متى كانت معالجتها أساسا، ممنوعة بموجب القوانين، كحال البيانات الحساسة. ومن واجب المسؤول عن المعالجة، متى كان الطلب مشروعا، أن يبادر إلى تنفيذ العملية المطلوبة.

وانسجاما مع مبدأ شرعية البيانات، لا يمكن السماح بمعالجة البيانات الشخصية، إلا إذا تم الحصول على إذن الشخص المعني، أو كان الأمر ضروريا لتنفيذ التزام قانوني، يكون الشخص المعني طرفا فيه، أو لتنفيذ موجب قانوني، أو ضروريا، لتنفيذ مهمة ذات منفعة عامة، يقوم بها المسؤول عن المعالجة، أو الجهة التي سلمت إليها المعلومات، أو أن يكون ضروريا لتنفيذ مصلحة شرعية للمسؤول عن المعالجة، أو الجهة التي سلمت إليها المعلومات، وشرط إلا يؤدي ذلك، إلى الأضرار بالحقوق الأساسية للشخص المعني.

بينما تنص المادة 12 من الإرشادات الأوروبية، على حق الشخص المعني بطلب التصحيح، والمادة 14 على حقه في الاعتراض. وهكذا يؤمن التقاء المواد الثلاث، الإطار القانوني، والأساس لحق التصحيح.

وكان المشترع التونسي، قد اقر ممارسة هذا الحق، في مواجهة السلطات العامة، في المادة 55 منه، حين اقر حق الشخص المعني، أو ورثته، التقدم بطلب التصحيح، وفرضه كموجب على السلطات العمومية، والجماعات المحلية، والمؤسسات العمومية، التي تعالج بيانات شخصية عائدة، للأمن العام، أو الدفاع الوطني، أو الملاحقات الجزائية.

وتماشيا مع ما تقدم، تنظر السلطات المذكورة، في الطلب المقدم، لتعديل البيانات، أو تيويمها، أو استكمالها، أو شطبها، في حال تم إعلامها، عن وجود شوائب فيها، وذلك بأية وسيلة تترك أثراً كتابيا.

- **الحق في الوصول إلى المعلومات**

يفترض إقرار حق الوصول إلى المعلومات، إمكانية الاطلاع عليها، من قبل صاحبها، الذي يحق له، طلب نسخة من المسؤول عن معالجتها، والحصول على جواب، حول ما إذا كانت بياناته، داخلة في عملية المعالجة، وأهداف هذه العملية، وفئات البيانات المعالجة، والجهات التي تسلم، أو تنقل إليها، لاسيما في حال انتقال هذه البيانات إلى دولة أخرى، أو إلى شركات في هذه الدول.

ويتخذ الرد على هذا الطلب، الشكل الخطي. وتقر بعض القوانين، كالقانون الفرنسي مثلا، حق صاحب البيانات، في الاطلاع على ما تجمعه الإدارات الرسمية عنه؛ كأجهزة الأمن والدفاع، أو غيرها، وذلك عبر طلب يتقدم به، إلى الهيئة الوطنية لحماية البيانات، التي تقوم بهذا الاطلاع، والرد على صاحب البيانات.

وينحصر الحق في الوصول إلى البيانات الشخصية، في حق الشخص المعني، بالوصول إلى معلوماته، ولا يشمل حق الاطلاع على بيانات أشخاص ثالثين، ولا أية تعليقات أو تحليلات قانونية لها، إلا إذا كانت هذه الأخيرة تحتوي هي الأخرى، على بيانات شخصية.

فإذا كانت الوثائق الإدارية المطلوب الوصول إليها، لا تحتوي بيانات شخصية، يصبح الحق في الوصول إليها، خاضعا لنظام قانون الحق في الوصول إلى المعلومات، الذي يعتبر أساسيا في آليات مكافحة الفساد، عبر إقرار حق المواطن في المعرفة والاطلاع، والمشاركة في الحياة العامة، وواحدا من العوامل الأساسية، في تعزيز الديمقراطية، عبر قيم المحاسبة، والشفافية، والمساءلة.

آلية التنفيذ: سلطة الرقابة

لا يعتبر الإطار القانوني فاعلا، إلا متى تأمنت آليات، وإمكانات التنفيذ الفاعل، والرقابة على التطبيق السليم للقانون. من هنا، يمكن القول، أن حماية البيانات الشخصية، لا تستقيم، بدون إنشاء جهاز إداري متخصص، يشرف على تطبيق قواعد، وأحكام القانون، وفقا للمبادئ والأهداف المعلنة فيه.

كذلك، يعتبر إنشاء مرجعية، تتولى السهر على تطبيق قوانين الحماية، دليلا على النية الجدية في الحماية، وعلى وعي الحكومة المعنية، بخصوصية مسألة حماية البيانات، في زمن إمكانات المعالجة الهائلة، والتقنيات المتخصصة، التي تستوجب، إضافة إلى وجود القانون والإلمام بمبادئه، إلماماً بتقنيات البرامج، والتطبيقات الرقمية، ورؤية واضحة وشاملة، تسمح بمعالجة التحديات، التي يثيرها هذا القطاع، في وجه القطاعات الأخرى، وحماية المكتسبات الإنسانية، على مستوى الحقوق والحريات.

ويترجم ذلك على المستوى العملي، بتكوين الهيئة من عدد من الأعضاء، من خلفيات مهنية، وعلمية، وخبراتية، يمكنها التعامل، مع الامتدادات المتنوعة، والانعكاسات المختلفة، لظاهرة معالجة البيانات الشخصية.

وكان البروتوكول الملحق بالاتفاقية الأوروبية لحماية الأشخاص، في مواجهة معالجة البيانات الشخصية آليا[157]، قد نص على التزام الدول المنضمة إليه، بإنشاء سلطات إشراف، تمارس مهماتها باستقلالية تامة، كعامل من عوامل تأمين حماية فاعلة للأفراد، في مواجهة معالجة البيانات الشخصية. وتكون هذه السلطة مسؤولة، عن مراقبة مدى الالتزام، بمندرجات الاتفاقية رقم 108.

بالرغم من اهتمامها بلحظ أحكام خاصة بإنشاء سلطة لحماية البيانات الشخصية، خالفت القوانين العربية، مبدأ استقلالية الهيئة، لناحية خضوعها الإداري، أو المالي.

[157] - www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181

وقد توافقت القوانين المذكورة، على مستوى إقرار معظم الاختصاصات والصلاحيات، الخاصة بالسلطة المولجة السهر على حسن تطبيق وتنفيذ القانون، بشكل ينسجم مع الدور المطلوب منها. فأنيط بها، تلقي التصريح عن المعالجات، ومسك وإدارة المعلومات الخاصة بالجهات المسؤولة عن المعالجة، وإعلام الجمهور بالمعالجات التي تتم. كما أعطيت حق الإدلاء برأيها، أمام الحكومة، والبرلمان، وأية جهة مختصة أخرى بوضع مشاريع إنشاء بيانات شخصية، وذلك في الأمور التي تتعلق بمشاريع ومقترحات القوانين، أو مشاريع النصوص التنظيمية، ذات الصلة بمعالجة البيانات الشخصية، سواء منها ما يتعلق ببعض فئات البيانات الحساسة، أو الأمن، أو الإحصاء، أو إجراءات معالجة البيانات.

وفي هذا الإطار، أقر المشترع المغربي، إنشاء لجنة وطنية لمراقبة حمايات البيانات، تسمى اللجنة الوطنية، بحسب المادة 27، من القانون، إلا انه اخضع هذه "السلطة" ذات الشخصية المعنوية، المستقلة ماليا، وتيسيريا، إلى الوزير الأول.

بينما لحظ التشريع القطري، إيكال دور سلطة الحماية، إلى الوحدة الإدارية المختصة في وزارة الاتصالات، والتي يدخل في مهامها: اتخاذ الإجراءات اللازمة للحماية؛ لاسيما منها التنسيق مع أية مجموعة، أو جهة تعمل في مجال معالجة البيانات، بهدف تشجيع وتطوير التنظيم الذاتي، ونشر الوعي حول قانون حماية البيانات، وتطوير برامج التعليم والتدريب المتخصصة.

كما تتولى هذه الإدارة، العمل مع المنظمات والجمعيات، لتعزيز سلامة الأطفال على الإنترنت، وتهتم بالأبحاث ورصد التطورات التقنية، وإعداد التقارير والتوصيات، بشأنها. وتعتبر تبعية هذه الجهة، غير متناسبة مع الدور المطلوب من سلطة حماية البيانات الشخصية، المضطلعة بمراقبة تطبيق أحكام وقواعد حماية البيانات.

إضافة إلى ما تقدم، نص المشترع التونسي، على إنشاء الهيئة الوطنية لحماية المعطيات

الشخصية، في الباب السادس منه، كسلطة تتمتع بالشخصية المعنوية، والاستقلال المالي، ليعود ويلحق موازنتها بموازنة وزارة حقوق الإنسان، وفي هذا، انتقاص واضح من استقلاليتها. أما فيما يتعلق بمهامها، فقد أسند إليها، مهمة إعداد قواعد سلوكية، وأنشطة التدريب، والتعليم، في مجال حماية البيانات الشخصية.

وكان التشريع الإماراتي[158]، قد أنشأ مؤسسة بيانات دبي، التي أسند إليها الإشراف، على تطبيق أحكام القانون والقوانين الصادرة بموجبه، وإعداد، وتحديث استراتيجية الحكومة الخاصة ببيانات دبي، والخطط والبرامج المتصلة بها، والإشراف على تطبيقها، بالتنسيق مع مركز دبي للأمن الإلكتروني، واقتراح القوانين والسياسات الخاصة بنشر وتبادل البيانات، بالتنسيق مع المركز بما يتواءم مع السياسات والخطط الاستراتيجية للإمارة، ورفعها إلى السلطات المختصة لاعتمادها.

كما أوكل إليها، متابعة التزام مزودي البيانات بالسياسات المعتمدة في شأن نشر وتبادل البيانات، سواء على مستوى العمليات أو المستويات الفنية، وتوحيد سياسات وخطط نشر وتبادل البيانات في الإمارة، ودعم أهداف الإمارة الرامية لجعل دبي مدينة ذكية.

على خط متصل، أسندت إلى المؤسسة، مهمة إبرام الاتفاقيات، ومذكرات التفاهم، مع الجهات المعنية بمعالجة البيانات، داخل الإمارة أو خارجها. إضافة إلى ذلك، تضطلع المؤسسة، بمهمة توعوية، من خلال عقد الدورات التدريبية، وورش العمل المتخصصة، حول نشر وتبادل البيانات، وتتولى التنسيق مع مركز دبي للأمن الإلكتروني، لإصدار القرارات المناسبة، بشأن معالجة البيانات، علاوة على قيامها بالتحقيق في الشكاوى والمخالفات بشأن مدى التزام مزودي البيانات، بأحكام قانون حماية البيانات، والقرارات الصادرة بموجبه، واتخاذ الإجراءات والتدابير اللازمة بشأنها، ووضع الحلول المناسبة.

---

[158] - قانون إنشاء مؤسسة بيانات دبي رقم (2) لسنة 2016.

- **استقلالية السلطة**

بشكل عام، تنشأ الهيئة، أو اللجنة المختصة بحماية البيانات، كجهاز إداري مستقل، نظرا لطبيعة مهامها، ولدورها القيادي، الموجه، الموضوعي، المشرف، التوعوي، والقضائي، من جهة أولى، ولطبيعة الصلاحيات التي تعطى لها، لتحقيق الهدف من حماية البيانات الشخصية، المحفوظة في ملفات ورقية، أو رقمية، في القطاعين العام والخاص، من جهة ثانية. يضاف إلى ذلك، ضرورة أن تتخذ قرارتها، وتصدر توصياتها، بشكل مستقل عن أية سلطة وصاية، يمكن أن تؤثر عليها، وان إدارياً.

من وجهة نظر قانونية، الهيئة سلطة عامة، وتكون، لهذه الغاية، جهازا له استقلالية القرار، والعمل، والتأثير في قطاع محدد، ومتخصص. وهي إدارة مستقلة؛ ما يمنح قراراتها الطبيعة الإدارية، التي تتمتع بها قرارات السلطات العامة، وبحيث يتم الطعن بها، أمام محاكم القضاء الإداري.

أما لناحية استقلاليتها، فتتجلى على مستويين: الأول، هو عدم خضوع أعضائها إلى الهرمية الوظيفية والإدارية، والمتبعة في الوزارات، كما انهم لا يتلقون أوامر، أو آراء، أو تعليمات من أية وزارة، أما الثاني، فهو حصانة أعضائها، لجهة عدم إمكانية عزلهم، ولجهة القواعد، التي تمنع ممارستهم لأية وظيفة أو نشاط، يمكن أن يتعارض مع عضويتهم في الهيئة.

فلا يجوز لرئيس الهيئة أو لأعضائها، أن يكونوا من الموظفين، أو من أصحاب المصالح في المؤسسات، أو الشركات العاملة في مجال الاتصالات ومعالجة البيانات. كما لا يجوز، أن تتوافر لهم أية مصالح في مؤسسة تمارس هذه الأنشطة، سواء أكان ذلك بصورة مباشرة، أم غير مباشرة.

وكانت التوصيات الأوروبية، الصادرة في العام 1995، قد نصت على استقلالية هيئات حماية البيانات الشخصية، كعامل أساسي، لا يمكن التنازل عنه. وقد ورد

ذلك في المادة 28 من الاتفاقية[159]، حيت شدد النص، على أن تعمل الهيئة، أو الهيئات التي تعينها الدولة، للإشراف على تطبيق قوانين حماية البيانات، باستقلالية تامة.

- أعضاء السلطة

غالبا ما يعين أعضاء الهيئات المستقلة، بمراسيم تتخذ من قبل السلطة التنفيذية؛ رئيس الجمهورية، أو مجلس الوزراء. لكن تعيين أعضاء هيئات الرقابة على حماية البيانات، يتم بحسب قواعد مختلفة، تبعا للبلد. ففي كثير من الأحيان، يتم تعيين الهيئة المكلفة بالحماية، من قبل السلطة التشريعية، وهذا أفضل بكثير، من تعيينها من قبل السلطة التنفيذية.

تختلف أنظمة التعيين، باختلاف المهمات المطلوبة من أعضاء الهيئة. فتخضع الهيئة المستقلة، مثلا لسيطرة البرلمان، وتكون له سلطة الاعتراض، أو حق النقض المعلل، ضد قرار الحكومة تعيين الأعضاء. وتعطي بعض القوانين صلاحية تعيين رئيس الهيئات المستقلة، إلى رئيس الجمهورية، كإيطاليا على سبيل المثال.

كما يمكن، أن تكون التعيينات سياسية، في بعض الحالات، كما يحدث في الولايات المتحدة الأميركية، مع ما يحمله هذا النوع، من مخاطر تعيين أعضاء لا يتمتعون بالكفاءة المطلوبة، في مقابل بلدان لا يمكن أن يتم التعيين فيها، إلا بناء على تحديد صارم للصفات والمؤهلات المطلوبة، التي تحددها القوانين، وبالتالي، لا يكون للجهة التي تعين، أية قدرة فعلية على الاختيار، وجل دورها ينحصر في الموافقة.

ففي إنكلترا مثلا، يعين الأعضاء، من بين أصحاب الخبرة، ومن شخصيات مستقلة عن السلطة السياسية، التي تتولى الحكم. بينما تلحظ بعض البلدان، تعيين شخصيات

[159] - Article 28 Autorité de contrôle
1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies.

سياسية، غير مؤيدة بالضرورة للسلطة الحاكمة؛ كوزراء، أو برلمانيين سابقين. وتميل الدول عامة، إلى تعيين الأعضاء، من بين الأشخاص الذين يقدمون ضمانا للاستقلالية، ويستوفون الشروط المطلوبة، لممارسة أعلى الوظائف الإدارية، أو القضائية، أو يملكون خبرات وكفاءات، تمكنهم من إنجاز المهام المطلوب تنفيذها، بحسب معايير موضوعية، دون انحياز، استنادا إلى قاعدة استقلالية القرار.

ويمكن للنظام المعتمد للتعيين، أن يكون مرنا، بحيث يلحظ تعيينا من قبل السلطتين التشريعية والتنفيذية، بناء على اقتراحات من الإدارات المختصة، إضافة إلى طريقة أصيلة ومباشرة، عبر الانتخاب، من أعضاء هيئة معينة، أو من بقية الأعضاء، كما يحصل في بعض القوانين، مع اختيار رئيس هيئة الرقابة على حماية البيانات. وبشكل عام، من المفترض اختيار الأعضاء، بناء على انتمائهم المهني، أو الوظيفي، أو المهارات المتوفرة، ويعزز هذا الأمر، من خلال التشاور مع الجهات، التي ينتمي إليها المعنيون.

- **سلطات الأجهزة المكلفة بالرقابة**

تتميز الهيئات المستقلة بسلطتها المعنوية، أكثر مما تتميز بالنفوذ الحقيقي التي تقره لها النصوص، لاسيما في البلدان الانجلوساكسونية. فيكون لها سلطات سياسية؛ بمعنى إنها تتمتع بوظيفة "الشرعية الاستراتيجية"، لهذه الغاية، إضافة إلى صلاحيات لتوجيه السياسة الإدارية، أو الاقتصادية، أو غيرها من السياسات، التي تقرها الحكومات.

ويكون لها في أنظمة أخرى، ثلاثة أنواع من السلطات، والتي يمكن، دمجها وممارستها:

- سلطة التحقيق مع الإدارات في القطاعين العام والخاص، والتي يمكن أن تصل إلى حدود ممارسة سلطات المقاضاة.
- سلطة التنظيم لقطاع ما، من خلال إقرارها مبادئ توجيهية عامة، أو معايير

محددة ودقيقة، تتسم غالبا بطبيعة تقنية متقدمة للغاية، كما يحصل في مجال تنظيم الاتصالات السلكية واللاسلكية، حيث تضطلع الهيئات الناظمة للاتصالات، بمهمة تنظيم المجالين السمعي البصري.

- سلطة إنزال العقاب، حيث تقر لها صلاحية إقرار عقوبات إدارية، وشبه قضائية، فيكون لها اختصاص لحل النزاعات، التي تقع عادة في نطاق صلاحية السلطة القضائية.

- **دورها: الجهة الناظمة لحماية البيانات**

هكذا، وبناء على الأحكام التي ترعى إنشاءها، ومهامها، وصلاحياتها، تضطلع الهيئة الوطنية لحماية البيانات الشخصية، بدور رئيسي، هو مواكبة من يقومون بمعالجة البيانات الشخصية، لمساعدتهم على الالتزام بإحكام القانون، ومساعدة أصحاب البيانات في ممارسة الحقوق، التي يقرها لهم، هذا من جهة أولى.

كما تلعب، من جهة ثانية، دور الجهة الناظمة لمعالجة البيانات، من حيث دراستها لتأثير التطورات التقنية، واستخداماتها، على الحياة الخاصة، والحريات، واهتمامها بوضع الأطر التنظيمية الأنسب، والأكثر فاعلية، لضمان خصوصية الأفراد، وحرياتهم، في مواجهة المخاطر الناشئة، والمستجدة. وتتوزع هذه المهام، على ما هو إداري، وإعلامي، وتنظيمي، ورقابي، وقضائي، واستشرافي.

في المقابل، يفرض القانون الذي ينشئ الهيئة، على المسؤولين عن المعالجة، ومنفذي العمليات، كما المتعاقدين معهم، التعاون مع الهيئة، وتنفيذ تعليماتها، وتسهيل مهماتها. كما يعتبر عرقلة عمل الهيئة، جرما يلاحق عليه بمقتضى القوانين المرعية الإجراء، لاسيما منها، القانون الجزائي، وحيث تطبق الأحكام التي تتعلق بعرقلة عمل السلطات العامة، وتحقيق العدالة.

ويقع على المؤسسات المعنية، موجب عدم اعتراض عمل الهيئة، لاسيما عندما تكون الزيارة لاماكن العمل، بإذن من القاضي المختص. كذلك، يتوجب إعطاء الهيئة، عبر من تنتدبهم للتحقيق، المعلومات المطلوبة، والامتناع عن إعطاء معلومات مغلوطة، أو تسليم وثائق غير صحيحة، أو ناقصة.

» في الإعلام والحماية

تتمحور هذه المهمة، حول تعزيز استخدام التقنيات، بطريقة تحمي الخصوصية، عبر تشجيع تقنيات التشفير. وتقوم لهذه الغاية، بتوفير المعلومات الضرورية، للمهنيين وأصحاب البيانات، على السواء، لفهم مندرجات القانون، وموجبات الحماية والأمن، والإحاطة بكافة إمكانات وأوجه ممارسة الحقوق، وأساليب تفعيلها.

وتعد لهذه الغاية، مواد تعليمية، كما تحفز أنشطة تربوية وتوعوية، وتصدر منشورات، أو كتيبات إرشادية، يمكن أن توجه، لفئات مختلفة، كالمستخدمين العاديين، أو المسؤولين عن المعالجة، أو أرباب العمل. كما تتفاعل الهيئة مع المعنيين، من مهنيين، وأفراد عاديين، عبر تدخلها المباشر، في حال بروز صعوبات، على مستوى تطبيق القانون.

» المواكبة وتقديم المشورة

تهتم الهيئة، بشكل خاص، بمرافقة المهنيين، ومساعدتهم على التقيد بأحكام قانون حماية البيانات، عبر تبسيط بعض القواعد الإجرائية، وشرح تقاطعات القوانين المرعية الإجراء، والآراء الفقهية، وبعض قرارات الاجتهاد. كما تبدي رأيها في مشاريع القوانين، والتعديلات، أو النصوص التنظيمية، التي تؤثر، أو تطاول حماية البيانات الشخصية.

وكانت المادة 28 من التوصيات الأوروبية الصادرة عام 1995، قد ألزمت الدول الموقعة، بمراجعة هيئة حماية البيانات، في كل مرة تلجأ فيها إلى اتخاذ تدابير إدارية، أو وضع نصوص تنظيمية، يمكنها أن تؤثر على حماية البيانات الشخصية، والحقوق والحريات[160].

وتصدر الهيئة، التوصيات إلى الحكومة، والمشترعين، كما تجيب على الأسئلة التي توجه إليها، حول الخطوات الواجبة، لضمان الالتزام بالقانون. وتعمد الهيئة، إلى إصدار معايير ومقاييس مرجعية للحماية، يمكن الاعتماد عليها، لتقييم مدى الالتزام، وصحته، كما تعطي رأيها في العقود التي تنجز لنقل البيانات، أو لتنفيذ عملية المعالجة، لدى جهات خارجية.

» سلطة التأديب

تستمد الهيئة هذه السلطة، من فلسفة وجودها، كسلطة إشراف. ويمكنها لهذه الغاية، تكليف عدد من أعضائها، بالتحقق من مدى التزام المؤسسات، والشركات المعنية بمعالجة البيانات الشخصية، بإحكام القانون، وباحترام حقوق الأفراد وحرياتهم. وتتم هذه المهمة، سواء عبر الإشراف المباشر، والتحقيق في مركز المعالجة، أو من خلال الاتصال هاتفيا، بالمسؤول عن المعالجة.

وتقوم الهيئة، بتحديد عدد من الضوابط، لتعمل بموجبها، على النظر في ما يقدم إليها من شكاوى، وما يعرض من قضايا. وتتمتع الهيئة، بصلاحية الدخول إلى أي جزء من المبنى، الذي تتم فيه معالجة البيانات، أو إلى الأجهزة، والأنظمة، والبيانات المعالجة، وسماع الأشخاص العاملين، والمسؤولين، على السواء، واستجواب من ترى في سماعه فائدة للتحريات، والتحقيقات، التي تجريها. كما يمكنها طلب نسخ،

---

[160] - Article 28 Autorité de contrôle
2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

عن أية وثائق ترى حاجة إليها. وغني عن القول، أن جميع أعضاء الهيئة، ملزمون بالحفاظ على سرية المعلومات، التي يطلعون عليها، بمناسبة قيامهم بأعمالهم.

وتلعب الهيئة دورا محفزا، حيث من المفترض، أن يجري تبليغها، قبل إنشاء أي ملف للبيانات الشخصية. علما أن القواعد الأوروبية الجديدة، ألغت هذا الموجب، مشددة بالمقابل، على موجبات الالتزام بالقانون، واتخاذ إجراءات الحماية، والأمن، واحترام حقوق الأفراد. وتتولى الهيئة، إصدار إشعارات رسمية، وتوجيه تنبيهات إلى المسؤول عن المعالجة، وإنزال عقوبات مالية، أو وضع اليد، وإيقاف المعالجة، وسحب الترخيص، في المعالجات التي يفرض القانون الحصول على ترخيص بشأنها، وفي حال الانتهاكات الخطيرة، للحقوق والحريات. كما تتولى الهيئة، تبليغ النيابة العامة، في بعض الحالات، والطلب من القضاء المختص، اتخاذ التدابير المناسبة، والضرورية.

» قمع المخالفات

تتفق جميع القوانين، على إقرار عقوبات على مخالفة أحكام حماية البيانات. تتنوع هذه المخالفات، بين ما هو متعلق بالمعالجة والجمع، وما يختص بنظام الحماية، وما يشكل اعتداء على حقوق الأشخاص المعنيين.

وتكون المخالفات مقصودة، أو عن إهمال، كعدم احترام إجراءات التبليغ، أو الحصول على التصريح المفروض، ومتابعة معالجة البيانات، دون احترام الإجراءات المفروضة، أو الاحتفاظ بالبيانات، لمدة تتجاوز تلك المعلن عنها، أو سوء الاستعمال، أو جمع البيانات بطريقة احتيالية، أو غير شرعية، أو غير شريفة.

وتتراوح العقوبة، بين الغرامات المالية، والسجن. وكانت القواعد الأوروبية الجديدة، قد شددت العقوبات، على عدم احترام القانون. وتتميز العقوبات التي أقرت في المادة 83 منها، بطبيعتها الرادعة، وتدرجها، بطريقة تتناسب والمخالفات المرتكبة.[161]

[161] - L’article 83 du RGPD stipule que des sanctions effectives, proportionnées et dissuasives seront délivrées pour toute violation du RGPD.

فبحسب النص، يمكن أن تصل قيمة العقوبة، إلى 4% من العائد السنوي لعمل الشركة، أو إلى 20 مليون يورو، في حال وقوع انتهاكات خطيرة، للموجبات الأساسية التي تقرها القواعد، مع اعتماد الحد الأعلى، ضد الشركات التي لا تلتزم الموجبات المفروضة، لجهة تمكين المواطن أو المقيمين، من استعادة زمام المبادرة، في إدارة بياناتهم الشخصية، منعا لانكشاف ما لا يريدون كشفه، من خصوصياتهم.

» الاستشراف

تشكل الهيئة نوعا من جهاز توعية، ومراقبة، للتطورات التقنية، والممارسات التجارية، أو الاجتماعية والمهنية، يمكن من خلاله، تحليل العوامل الخطرة، ومصادر التهديد للحقوق والحريات.

وتقوم الهيئة، لهذه الغاية، بتجربة التطبيقات والبرامج الجديدة، بواسطة العاملين فيها، بما يساهم في رصد الأخطار المحتملة، وفي تطوير تقنيات الحماية، والحفاظ على الخصوصية. لذلك، تعمد إلى التعاون مع القطاعين العام والخاص، ومع الشركات المنتجة للبرمجيات، والأجهزة الإلكترونية، بشكل خاص، فتقدم المشورة لها، حول تصاميم الخصوصية، وإجراءاتها.

وتحقيقا لتعاون مثمر وفاعل، تنظم الهيئة نشاطات علمية، ولقاءات، حول المواضيع التقنية، والتنظيمية، والقانونية، الخاصة بحماية الخصوصية، والحريات، بما يجعلها تلعب دورا قياديا، على مستوى إقرار بعض شرع أخلاقيات استخدام التقنيات، وإنتاجها.

- تعيين أعضاء سلطة الرقابة

يعين أعضاء سلطة الرقابة على معالجة البيانات الشخصية، من بين شخصيات مشهود لها بالكفاءة العلمية، والوظيفية، وغالبا ما يتم اختيارهم، من قبل السلطات التشريعية

والتنفيذية، والمهنية، المعنية بتطوير قطاع الاتصالات والمعلومات. ويحرص في تأليف هذه السلطة، على تغطية اكبر عدد ممكن من الاختصاصات، وعلى ضمان احترام التعددية، من خلال دمج الحد الأقصى، من الآراء والتوجهات، والخبراء، أو ممثلي القطاعات المعنية.

ينتخب رئيسها، من قبل الأعضاء المعنيين، بحيث لا يكون لأية سلطة في الدولة، تأثير مباشر، داخلها، من خلال هذه العملية. ويمنع على الأعضاء، كما على الرئيس، ممارسة أي نشاط، أو امتلاك أية مصلحة، أو منفعة، في قطاع خدماتي، أو صناعي، أو وظيفي، بما يمكن أن يؤثر على موضوعيته، ومصداقية مشاركته في قرارات الهيئة. ويعتبر هذا الأمر، من العوامل، التي تساهم في تحصين استقلاليتها.

ويمكننا القول، أن القوانين العربية قد لحظت، كما هو واضح من النصوص الخاصة بتعيين أعضاء سلطة الرقابة، أهمية استقلالية الأعضاء، ودور غياب المصلحة المباشرة، أو غير المباشرة، في التأثير على قراراتهم، وان بدرجات مختلفة.

فقد أسند التشريع المغربي، مهمة اختيار الرئيس وتعيين الأعضاء، إلى الملك، على ان يتم اقتراح الأعضاء الستة، من قبل الوزير الأول، ورئيس مجلس النواب، ورئيس مجلس المستشارين. وقد حظرت المادة 35، على أعضاء الهيئة، الجمع بين وظيفة عامة، أو عضوية مجلس إدارة، في شركة تتعاطى معالجة البيانات الشخصية. كما نص على حالات تعارض، كحالة استبعاد العضو من المداولات، أو عمليات التحقيق، في نشاطات شركة ما، ما لم تمض فترة خمس سنوات، على تاريخ تركه العمل فيها.

وكان المشترع المصري، قد ترك هو الآخر، تعيين رئيس جهاز حماية البيانات، لرئيس مجلس الوزراء، إضافة إلى نائبين له، يتم اختيارهما من نواب رئيس مجلس الدولة. وكانت المادة 35 منه، قد نصت على تشكيل مجلس إدارة جهاز الرقابة،

وتحديد المعاملة المالية لرئيسه، ونائبه، وأعضائه، بقرار يصدره رئيس مجلس الوزراء، بناء على ترشيح الوزير المختص.

بينما نص القانون الموريتاني، على السماح لعضو السلطة، ما عدا الرئيس، بممارسة نشاطات أو وظائف أخرى، لكن شرط ألا يكون وزيرا في الحكومة، أو مدير المؤسسة، أو مالكا لأسهم في مؤسسات قطاع المعلوماتية والاتصالات الإلكترونية، تاركا تشكيل وتعيين الأعضاء، لمرسوم يصدر لاحقا.

كما فرض القانون على جميع الأعضاء، التصريح عن المصالح المباشرة، أو غير المباشرة، التي يملكونها، أو ينوون امتلاكها، وعلى الوظائف التي يمارسونها، أو ينوون ممارستها، لدى أية مؤسسة.

وقد تميز هذا القانون، بفرضه موجب تأدية اليمين، على الأعضاء، وذلك، أمام المحكمة العليا مجتمعة في جلسة رسمية، يتعهدون فيها، بتأدية وظيفتهم بأمانة وإخلاص، وبكل استقلالية، وحياد، ونزاهة، وبان يحافظوا على سرية المداولات. كما يلتزم بأداء اليمين، كل من تختارهم السلطة نفسها، فيما بعد، لمساعدتها في مهامها.

واعتبر القانون، أن لأعضاء سلطة الحماية حصانة، تمنع عنهم أي تعرض، نتيجة آرائهم، وذلك خلال فترة وظيفتهم. وعليه، فقد جمع المشترع المغربي، بين اليمين، التي تؤدى في المجال القضائي، أو بعض المهن الحرة كالطب، وبعض ميزات الممثل التشريعي، كالحصانة، ما يدعم فرص ممارستهم لمهامهم، واتخاذ القرارات اللازمة، بحرية واستقلال.

إضافة إلى ما تقدم، كان التشريع التونسي، قد اخضع تعيين رئيس السلطة وأعضائها، "لصدور أمر"، وابرز في المادة 18 منه، خلفيات تركيبتها، حيث توزعت على ممثلين للوزارات المعنية بالأمن، كالدفاع والداخلية، وتلك المعنية بحماية الحقوق والحريات، كالهيئة العليا لحقوق الإنسان والحريات الأساسية، والصحة العمومية،

والبحث العلمي، إضافة إلى المختصين في مجال التكنولوجيا والاتصالات، والقضاة، وأعضاء من البرلمان، ومجلس المستشارين، والوزارة الأولى.

مفوض حماية البيانات

سنتطرق إليه، في إطار التشريعات الأوروبية، ومن ثم من خلال القوانين العربية.

- **القوانين الأوروبية**

إن مفوض حماية البيانات في القانون الأوروبي، هو الشخص المسؤول عن حماية البيانات داخل المؤسسة، التي تقوم بمعالجة البيانات الشخصية. أما المهام الأساسية المنوطة به، فهي تلك التي تقوم على مراقبة التزام المؤسسة، أو المنظمة، أو الادارة التي يعمل لديها، بتطبيق النصوص القانونية الخاصة بحماية البيانات، من جهة، وبالقواعد الداخلية للمؤسسة، من جهة أخرى. كما يدخل في مهامه، موضوع تقديم الاستشارة، وتأمين الاتصال بين المؤسسة، والسلطة الوطنية المخولة الإشراف على تطبيق قوانين حماية البيانات.

ويعتبر تعيين هذا المفوض، حاليا، وبعد دخول التشريع الأوروبي الجديد حيز التنفيذ، من أفضل الخطوات، التي يمكنها أن تضمن التزام المؤسسات المختلفة، بأحكام حماية البيانات. أما تعيينه فهو اختياري، ما عدا الحالات التي ينص عليها القانون. وبالفعل، فقد نص التشريع الأوروبي الجديد، في المادة 37 منه، على إلزامية تعيين مفوض مسؤول لحماية البيانات، سواء بالنسبة للمسؤول عن المعالجة، أو للمعالج من الباطن، في حالات ثلاث، هي:

- المعالجة التي تتم بواسطة سلطة، أو هيئة عامة.
- عندما تكون الأنشطة الأساسية للمعالج المسؤول، أو المتعاقد من الباطن، ذات طبيعة أو نطاق، أو غاية، تفرض مراقبة منهجية، ومنتظمة، على نطاق واسع للأشخاص الطبيعيين المعنيين.

- عندما تكون الأنشطة الأساسية للمعالج المسؤول، أو المتعاقد من الباطن، تتناول معالجة بيانات ذات طبيعة حساسة (البيانات الصحية والبيانات البيومترية والآراء السياسية والمعتقدات الدينية ...) أو كانت البيانات موضوع المعالجة، بيانات خاصة بالأحكام الجزائية، أو المخالفات.

فإذا توقفنا عند الحالة الثانية، نلاحظ إنها تستدعي التمهل والتفكير، بمسألة الالتزام بموجب "المراقبة المنهجية والمنتظمة والواسعة النطاق". ففي عصر البيانات الضخمة، تعتبر البيانات الشخصية، أساسية في جميع الأنشطة، بما في ذلك أنشطة التجار الإلكترونيين، الذين يصنفون عملاءهم، من خلال استخدام ملفات تعريف الارتباط والتتبع، بهدف تقديم منتجات تتكيف وحاجاتهم؛ وتأتي ضمن هذه الفئة، شبكات المطاعم التي تقدم خدمات التوصيل، وشركات الإعلانات. فإذا اعتبر هؤلاء التجار، من أصحاب الأنشطة، التي تندرج ضمن الفئة الثانية، أصبح من الواجب عليهم تعيين مفوض لحماية البيانات.

وكانت مجموعة G29 قد اعتمدت تفسيرا موسعاً للأحكام التي نصت عليها القواعد الأوروبية الجديدة، بما يوسع دائرة المؤسسات أو المنظمات التي يفترض بها تعيين مفوض لحماية البيانات، بما في ذلك التجار الإلكترونيين الذين يستخدمون البيانات لتنفيذ عمليات التنقيب عن البيانات بشكل هادف ومحدد، لا سيما عبر استغلال أنظمة العضوية، والولاء على سبيل المثال، وعبر استهداف مجموع الأشخاص في قطاع سريع النمو، هو قطاع إنترنت الأشياء.

في هذا الإطار، نشرت مجموعة الـG29، التي تجمع هيئات حماية البيانات الأوروبية، بعض المبادئ التوجيهية، في إطار تحديدها للحالات التي تفترض تعيين مفوض حماية البيانات، والتي يمكن الاسترشاد بها. إلا أن هذه المبادئ لم تحدد الحالات، التي يعتبر فيها هذا الأمر إلزامياً، وذلك، عبر الاعتماد على بعض المعايير، ومنها:

• ارتباط معالجة البيانات الشخصية بـ "الأعمال الأساسية" للمنظمة. وكانت القواعد الأوروبية الجديدة، قد استخدمت هذا المصطلح في الفقرة 97 من الديباجة[162] للدلالة، على أنه "في القطاع الخاص"، تتعلق الأنشطة الأساسية لوحدة التحكم بأعمالها الأساسية، و لا تتعلق بمعالجة البيانات الشخصية، كنشاط إضافي.

والأعمال الأساسية بحسب المجموعة G29، هي الأعمال الأساسية في العمليات التي لا بد أن يقوم بها المسؤول عن المعالجة، أو المتعاقد من الباطن لتحقيق أهدافه، خاصة عندما تكون معالجة البيانات، جزءًا لا يتجزأ من أعمال المؤسسة.

فالعمل الرئيسي لمؤسسة الأمن والحماية، هو ضمان سلامة المباني، والقاطنين فيها. لكن تأدية هذه المهمة، تتطلب بشكل رئيسي، تجهيز الأماكن المستهدفة بكاميرات مراقبة، وتسجيل أسماء الأشخاص الذين يدخلون إليها، أو صور عن بطاقات هويتهم، وأرقام السيارات التي تستخدم المواقف التابعة لها، ما يجعل هذه المؤسسة، ملزمة بتعيين مفوض حماية للبيانات. ويشترط في هذا الأخير، أن يتمتع بمستوى من المعرفة الخاصة بمعالجة هذا النوع من البيانات الشخصية، وان يتمكن من أداء مهامه بشكل مستقل، سواء، أكان موظفا في الوحدة المسؤولة عن معالجة البيانات، أم لا.

ولا يتطلب الأمر تعيين مفوض لحماية البيانات، في حال كانت معالجة البيانات، مهمة تابعة للنشاط الأساسي للمؤسسة، كأن تتم معالجة البيانات، لإتمام كشوفات مستحقات العاملين، أو إدارة دوام العمل، ومتابعة تنفيذه بشكل مناسب.

وينطبق مفهوم "النطاق الواسع"، انطلاقا من نص الفقرة 91 من الديباجة، على عمليات المعالجة التي تطاول معالجة كميات كبيرة من البيانات الشخصية، على

[162] -Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - paragraphe 97-"Dans le secteur privé, les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire"
https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32016R0679

المستوى الإقليمي، أو الوطني، أو أبعد من ذلك، والتي تؤثر على عدد كبير من الأشخاص المعنيين، بشكل ينتج عنه مخاطر عالية، نتيجة طبيعتها الحساسة، عندما يتم تطبيق تقنيات حديثة على نطاق واسع، أو على عمليات معالجة أخرى، بما يرفع منسوب المخاطر بالنسبة لحقوق الأفراد وحرياتهم، لاسيما عندما تزداد صعوبة ممارستها، نتيجة هذه العمليات[163].

إضافة إلى ذلك، أقرت المجموعة G29، عددا من العناصر، التي لا بد من أخذها بعين الاعتبار عند مقاربة هذا المفهوم؛ كعدد الأفراد الذين تطاول المعالجة بياناتهم، وحجم البيانات، وأصنافها، ومدة المعالجة، واستمراريتها، والنطاق الجغرافي الذي تغطيه.

وكانت القواعد الأوروبية الجديدة، قد أخضعت لأحكامها، عمليات معالجة البيانات الشخصية التي تتم، من قبل مسؤول عن المعالجة، أو متعاقد من الباطن، غير موجودين على أرض الاتحاد الأوروبي، عندما تطاول هذه المعالجة، تصرفات الأشخاص الطبيعيين، ومتابعتها، داخل الاتحاد الأوروبي.

كما اعتبرت، أنه ومن أجل تحديد ما إذا كان يمكن اعتبار نشاط المعالجة، كمتابعة لسلوك الأشخاص المعنيين، من الضروري تحديد ما إذا كان الأشخاص الطبيعيين متابعين على الإنترنت، الأمر الذي ينطوي على إمكانية استخدام تقنيات معالجة البيانات لاحقاً، بطريقة تستخدم فيها تقنيات تحديد الأطياف، بهدف اتخاذ قرارات تعني الأشخاص الطبيعيين أصحاب البيانات، أو تحليل ميولهم، أو توقع ما يفضلونه، وتصرفاتهم، وإمكاناتهم الذهنية[164].

[163] - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données paragraphe 91 - Cela devrait s'appliquer en particulier aux opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ainsi qu'à d'autres opérations de traitement qui engendrent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces personnes d'exercer leurs droits"
https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32016R0679

[164] - paragraphe 24 du préambule

وقد حددت مجموعة الـG29، عددا من العوامل، التي يمكن لتوافر واحد منها، أو اكثر، أن يطبع المعالجة بصفة الانتظام، أو المنهجية. فاعتبرت الرقابة منتظمة متى تمت المتابعة خلال فترات معينة، أو متى كانت متكررة، أو منتظمة بحسب وقت معين، أو مستمرة، أو دورية. بينما اعتبرتها منهجية، متى تمت في إطار نظام محدد، ووفقا لطريقة منظمة، أو كجزء من الاستراتيجية المعتمدة، أو ضمن خطة أكثر عمومية، لجمع البيانات والرصد.

- **في القوانين العربية**

في القوانين العربية، التي تطرقنا إليها، لم يتم ذكر مفوض حماية البيانات، باستثناء ما ورد حول تعيين مفوض لحماية البيانات في قانون المركز المالي الدولي في دبي[165]، لحماية البيانات، وذلك بهدف التنسيق مع الجهات الدولية، التي يتم تبادل البيانات معها، والانسجام مع أفضل الممارسات العالمية، على ما جاء في إعلان أهداف القانون. مع العلم، إن هذا الأخير، لم ينشئ هيئة، أو سلطة وطنية مختصة لحماية البيانات، ولذا يمكن أن تكون نية المشترع، متجهة إلى إحلال اعتماد المفوض مكانها. وقد نصت المادة السابعة من قانون مركز دبي المالي الدولي، على إخضاع إدارة هذا القانون، لمفوض حماية البيانات[166].

وكذلك فعل المشترع الموريتاني،حيث اشترط تعيين مفوض للحكومة لدى السلطة، يلعب دور صلة الوصل بين السلطة والحكومة، يشارك في جميع جلسات السلطة، ويطلعها على توجهات الحكومة، ودوافع الإدارة المتعلقة بتطبيق المعالجات، ويكون له، الوضعية المماثلة لأعضائها، بيد انه لا يشارك في التصويت.

[165] - DIFC data protection law- cited as the "Data Protection Law 2007"
https://www.difc.ae/files/3615/1739/8803/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf

[166] - Art. 7. Administration of the Law This Law and any legislation made for the purpose of this Law is administered by the Commissioner of Data Protection.
https://www.difc.ae/files/3615/1739/8803/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf

خلاصة

يبدو جليا مما تقدم، أن مسألة حماية البيانات الشخصية، باتت مدرجة في سلم أولويات الدول عامة، حيث تحظى باهتمامات متفاوتة، وتوجب مواكبة دائمة للتطورات المتصلة بمعالجتها، ورصدا معمقا لآثار هذه العملية.

ففي كل يوم، تتزايد كمية البيانات الشخصية التي تعالج، ويخلق المزيد من وحدات التخزين، وتبتكر تقنيات وأساليب، لجمعها، وحفظها، واستثمارها. ومما لا شك فيه، إن جزءا هاما منها، لا يتعدى كونه بيانات عادية، لا ضير من جمعها. لكن الأكيد، أن تقنيات المعالجة الحديثة، التي يمكن أن تعالجها وتقاطعها، إلى جانب معلومات أخرى، تجعلها جد معبرة، وبالتالي، كاشفة ومهددة لخصوصياتنا، وحياتنا.

فالأدوات، والبرامج، والتطبيقات، وشبكات التواصل الاجتماعي، والحوسبة السحابية، أصبحت جزءا أساسيا، من الحياة اليومية لكل مواطن، وأداة لتسهيل عمل الأفراد، والأشخاص المعنويين، في القطاعين العام والخاص، وحولت تفاصيل الحياة اليومية لكل شخص طبيعي، إلى مصدر معلومات، ذي قيمة يعتمد عليها، في الاقتصاد الرقمي، والخدمات الإلكترونية، وتطوير عمل الهيئات، دون استثناء.

وفي هذا السياق، تشكل قوانين حماية البيانات الشخصية، والحقوق الأساسية للإنسان، الإطار الأنسب لمواجهة مخاطر المعالجة الإلكترونية لهذه البيانات. وتشكل الهيئات، التي تنشأ للإشراف على تطبيق احترام مبادئ المعالجة، وحقوق الأشخاص الطبيعيين، في مواجهة المخاطر التي تطرحها، التنظيم الإداري الأمثل، لضمان فاعلية هذه القوانين، والالتزام بها.

وفي عصر الاستراتيجيات الإلكترونية الوطنية، والإقليمية، والدولية، لم يعتمد عدد من الدول العربية، قانونا لحماية البيانات الشخصية، حتى اليوم، وذلك، بالرغم من الأهمية القصوى لاعتماد إطار قانوني مناسب، لاستخدام تقنيات المعلومات والاتصالات، يضمن حماية واحترام حقوق الأشخاص، الذين يعيشون فيها.

أما القوانين العربية التي عملنا عليها، فإنها تشكوا من ثغرات عدة، لاسيما لجهة آلية التنفيذ، حيث لم تعتمد المعايير المطلوبة، في تعيين أعضاء سلطة حماية البيانات، بما يضمن استقلاليتها، ويؤمن لها مستلزمات اتخاذ القرارات، بحرية تامة. وهذا يوجب بالتأكيد، على ضرورة الأخذ بما هو معمول به في التشريع الأوروبي، الذي يشدد على دور هذه السلطة، في حماية الأشخاص الطبيعيين من تجاوزات السلطات العام، والحفاظ على حقوقهم وحرياتهم، في مواجهة ممارسات الشركات الكبرى، التي تستثمر في بياناتهم، وتفقدهم السيطرة على حياتهم الخاصة. وفي سياق متصل، يفترض بالدول العربية، وعلى غرار ما هو معمول به، على المستوى الدولي، التنسيق فيما بينها، بما يؤمن الانسجام بين قوانين الحماية، لتأمين حماية البيانات على الصعيدين المحلي والدولي، ضمانا للتدفق الحر للبيانات عبر الحدود، وحماية الحقوق الأساسية للإنسان العربي.

إن اعتماد هذه المعايير، يحقق الانسجام المطلوب بين القوانين العربية، من جهة، وبينها وبين أفضل الممارسات العالمية، من جهة ثانية. كما يؤدي، إلى زيادة القدرة التنافسية لمزودي الخدمات فيها، وتأمين انتقال البيانات بشكل آمن وسلس، بما يدعم صعود مؤشرات القدرة التنافسية للدولة، على المستوى الدولي، وتعزيز الشفافية، وإرساء قواعد الحوكمة الرشيدة، في مجال نشر وتبادل البيانات والمعلومات؛ عبر إرساء قواعد التوازن بين عمليات معالجة المعلومات، ونقلها، وبين الحق في الحفاظ على الخصوصية، وسرية البيانات، وإمكانات ممارسة الحقوق والحريات.

كما تعزز قوانين حماية البيانات، إمكانات الاستثمار الأفضل لها، سواء من خلال استخدامها في ربط الخدمات الإدارية الرسمية، تسهيلا لأمور المواطنين، أو في تطوير خدمات القطاع الخاص، والتجارة الإلكترونية، والاقتصاد الرقمي، وغير ذلك، مما يساهم في دفع عجلة التحول الرقمي، بشكل ثابت وسليم.

ومما لا شك فيه، أن السبيل الأسلم، إلى الانسجام على المستوى العربي، يكون في إقرار اتفاقية عربية لحماية البيانات الشخصية، وإنشاء هيئة عربية خاصة، تضطلع بمهام التنسيق بين الدول، وتتولى وضع السياسات المشتركة، لحماية المواطنين العرب.



الدكتورة
منى الأشقر جبور

دكتوراه دولة في القانون الخاص، استاذ محاضر في الجامعة اللبنانية. متخصصة في المعلوماتية القانونية. محاضرة في العديد من المؤتمرات الدولية والعربية. وضعت منهجية لمعالجة البيانات القانونية، وشاركت في لجان المكنز في جامعة الدول العربية، وفي اعداد دراسة انشاء قواعد معلومات قانونية لحساب وزارة العدل الكويتية. رئيسة الجمعية اللبنانية لتكنولوجيا المعلومات، عضو مؤسس في المرصد العربي للامن السيبراني، مؤسسة مركز مكافحة الجريمة السيبرانية، عضو في الهيئة الدائمة للامن السيبراني في الاتحاد الدولي للعلماء، عضو في الفريق الفرانكوفوني للتوعية في هيئة ادارة اسماء نطاقات الانترنت (الآيكان) وفي منتدى حوكمة الانترنت.

مثلت لبنان في الهيئة الاستشارية الحكومية في الآيكان. صاحبة عدد من المؤلفات والمقالات باللغات العربية والفرنسية والانكليزية، في المعلوماتية القانونية، وقانون الانترنت، وحوكمة الانترنت، والقانون السيبراني، وحماية البيانات ذات الطابع الشخصي، والحق في الخصوصية. كلفت من قبل مركز البحوث القانونية والقضائية في جامعة الدول العربية، في العام ٢٠١٤ بوضع مسودة اتفاقية عربية للامن السيبراني. تعاونت مع عدد من المنظمات الدولية مثل الامم المتحدة والمنظمة الدولية للفرانكوفونية.




الدكتور
محمود عارف جبور

محمود عارف جبور حائز على دكتوراه دولة في العلوم السياسية والادارية، أستاذ محاضر في الجامعة اللبنانية، صاحب مؤلفات عديدة، في مواضيع مكافحة الارهاب، والوصول الى المعلومات، والأنظمة السياسية، والسياسات العامة، والادارة العامة، وفي مجال القانون السيبراني والسياسات السيبرانية، مشرف على رسائل جامعية تناولت موضوعات القوة في الفضاء السيبراني، والحياد، والصراعات السياسية في لبنان والعالم. عضو مؤسس في معهد الدراسات والتوثيق والابحاث اللبنانية (ايدريل) وعضو مؤسس في جمعية المركز اللبناني للمعلومات.



www.carjj.org